

# HOSPITAL AND HEALTHCARE SECURITY



Russell L. Colling  
Tony W. York

FIFTH EDITION



*Butterworth-Heinemann* is an imprint of Elsevier  
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA  
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

**© 2010 ELSEVIER Inc. All rights reserved.**

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions). This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

**Notices**

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

**Library of Congress Cataloging-in-Publication Data**

Application submitted

**British Library Cataloguing-in-Publication Data**

A catalogue record for this book is available from the British Library.

ISBN: 978-1-85617-613-2

Printed in the United States of America

08 09 10 11 12 13 10 9 8 7 6 5 4 3 2 1

For information on rights, translations, and bulk sales, contact Matt Pedersen,  
Commercial Sales Director and Rights; email [m.pedersen@elsevier.com](mailto:m.pedersen@elsevier.com)

Working together to grow  
libraries in developing countries

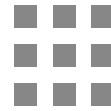
[www.elsevier.com](http://www.elsevier.com) | [www.bookaid.org](http://www.bookaid.org) | [www.sabre.org](http://www.sabre.org)

ELSEVIER

BOOK AID  
International

Sabre Foundation

For information on all Butterworth–Heinemann publications  
visit our Web site at [www.elsevierdirect.com](http://www.elsevierdirect.com)



# Acknowledgements

The authors are extremely appreciative of all the support and encouragement received during the preparation of this manuscript. This book would not have been possible without the contributions of our peers, colleagues, associates, and the International Association for Healthcare Security and Safety (IAHSS). It is difficult to keep track of all the healthcare security professionals who we have interacted with over the years that have challenged our thinking about the issues of safeguarding the healthcare environment and from whom we have learned so much. Healthcare Security is truly progressing in its transition into a profession that we can all be proud due to the contributions of so many. Our profound thanks to all of you who give so tirelessly to creating a safe environment where healing can occur.

We would also like to thank Pam Chester, acquisitions editor, and the entire Elsevier team for their encouragement to update this classic text. Their understanding of the changing healthcare security climate inspired Russ to tackle a fifth edition and add Tony as a coauthor.

As with all great teams, there has to be a driving force for each of us and we owe our deepest gratitude to the contributions and sacrifices made by our loving wives, Linda and Cara, during this long and arduous process. In the end, we could not have completed this manuscript without their understanding and support.



# IAHSS Healthcare Basic Security Guideline Placement

The authors have placed great emphasis on the IAHSS Guidelines in the fifth edition of *Hospital and Healthcare Security*. Below is a reference guide for where they are located in the text.

<b>Guideline</b>	<b>Title</b>	<b>Chapter</b>
01.01	Security Management Plan	4
01.02	Security Risk Assessments	3
02.01	Security Administrator	4
02.02.01	Targeted Violence	19
02.03	Forensic Patient Security	12
02.04	Security Role in Patient Management	12
02.05	Security Officer Use of Physical Force	8
02.06	Home Health Security	22
02.07	Security Officer Staffing & Deployment	6
02.08	Searching Patients and Patient Areas for Contraband	12
03.01	Security Officer Training	9
03.02	General Staff Security Orientation and Education	15
04.01	Investigations-General	16
04.02	Covert Investigations	16
05.01	Security Incident Reporting	11
06.01	Program Measurement/Improvement- General	4
07.01	Access Control-Identification System	14
08.01	Electronic Security Systems	18
08.02	Use of Closed Circuit Television (CCTV)	18
09.01	Security Sensitive Areas	20

(Continued)

*(Continued)*

<b>Guideline</b>	<b>Title</b>	<b>Chapter</b>
09.02	Infant/Pediatric Security	20
09.03	Security in the Emergency Care Setting	20
09.04	Patient Elopement	12
10.01	Emergency Management-General	24



# The Healthcare Environment

The only constant in today's healthcare environment is the dynamic challenges continuously facing healthcare administrators and those charged to protect the industry. Today's healthcare environment poses daily tests for security administrators charged with protecting these critical infrastructures. The delivery of healthcare changes rapidly and is vastly different from what it was just a few years ago. Hospitals are no longer an isolated group of free-standing buildings. They are critical infrastructures forming complex medical centers serving diverse patient populations with visitors traveling great distances to seek care and receive specialized medical treatment. It is not uncommon for medical centers and hospitals alike to find themselves as parts of a large healthcare system. These healthcare systems often have dozens of facilities-serving communities near the main facility, or they may be a part of system with facilities in many states removed. The competitive nature of healthcare has challenged administrators and security leaders alike to present a safe and secure environment that is coupled with an open, hospitality feel.

The current security landscape affects all types of organizations and all aspects of the healthcare industry. Heightened safety concerns following the 9/11 terrorist attacks have compelled government agencies, the healthcare industry, and commercial establishments worldwide to employ sophisticated security services. Alarmed by the vulnerability of their legacy systems, many organizations are upgrading to state-of-the-art security programs and systems, which include monitoring surveillance services and well-trained security ambassadors. This trend is likely to continue as healthcare institutions and various other establishments seek greater security due to growing workplace violence, changing patient populations (due to reduction of mental health reimbursement), employee thefts, corporate espionage, and the threat of terrorism.

The need for increased security has provided an unprecedented challenge in the methods and philosophies regarding protection of our healthcare organizations. Their safeguarding cannot be completely dependent on the security department. Many aspects of protecting healthcare organizations reach far beyond the control of the commonly accepted elements of a healthcare security department. Today, in order to achieve a high level of security, managers, top executives, and boards of directors must be more involved, through appropriate funding levels, with managing and supporting security issues. These leaders must accept a greater responsibility and ownership for security in their day-to-day management obligations.

Practically everyone uses healthcare, or has a close connection to someone who uses healthcare, in any given year. In 2006, the US's healthcare bill climbed above \$2 trillion. On average, healthcare consumes over \$7,000 per person per year—over one-sixth of the average American income.<sup>1</sup> Private funding provides 54% of this dollar amount, while public programs pick up the remaining 46%.

For more than two decades, the cost of healthcare has exceeded the general rate of inflation (or the rate of growth of the economy)<sup>2</sup> and is rising faster than wages. Much of these costs are incurred by the sickest patients. It is estimated that about 10% of the population accounts for more than 60% of healthcare costs.<sup>3</sup> Despite private, free-standing ambulatory care centers, declining patient days, long-term care facilities, wellness programs, and advances in outpatient and home care, hospitals remain the primary source of healthcare in terms of dollars expended.

The increased costs of providing healthcare is at least partly the result of the success of our healthcare delivery system—it is the result of larger number of people living to an older age and needing increasing amounts of care. There continues to be an explosive growth in the number of individuals with chronic conditions, a seemingly insatiable demand for emergency care services and intensive care, progressive expansion of applications for minimally invasive surgery and other procedures, and heightened concerns about inefficiency, access to care, and medical errors across the healthcare delivery system. A 2008 analysis by PricewaterhouseCoopers concluded that more than half of the dollars in the US \$2.2 trillion healthcare system are wasted. Medical errors, inefficient use of information technology, and poorly managed chronic diseases were all cited as factors. Dwarfing these reasons is a phenomenon in which doctors order tests to avoid the threat of a malpractice lawsuit—otherwise known as “defensive medicine.” At \$210 billion annually, defensive medicine is one of the largest contributors to waste. A 2005 survey in the *Journal of the Medical Association* found that 93% of doctors reported practicing defensive medicine.<sup>4</sup>

## Categories of Healthcare

Direct clinical care of patients is being delivered in all kinds of organizations and in all types of facilities. This diversity is generally the result of a particular entity wanting greater patient market share and is creating environments with low overhead to maintain cost control. A basic concept is to bring the delivery of care geographically closer to the patient. Lower unit costs are also intended to provide greater patient accessibility to quality care. This geographical spread of organizational facilities is based on the great amount of outpatient procedures once done only in the hospital. Healthcare can be viewed on a continuum from assisted living (low acuity) to acute care (high acuity). This progression follows these basic steps:

- **Assisted Living**—provides some help with day-to-day living activities, often including transportation services to healthcare delivery sites, some limited medical care presence in the living facility, and general staff watchfulness.

- **Home Care**—healthcare staff generally visit and provide care in the home with a coordinated plan of treatment and services.
- **Outpatient Services**—include surgery, clinic visits, physical therapy, psychological counseling, speech therapy, and dental care.
- **Intermediate Care**—provides 24-hour oversight and is often tied closely to geriatric care.
- **Skilled Care**—requires intervention skills by caregivers as opposed to caretakers.
- **Short-Term Acute Care**—is generally medically complex and includes post-surgical intensive rehabilitation, respirator care, and intensive oversight.
- **Acute Care**—occurs when a patient is medically unstable and includes extensive use of invasive procedures, high level of staff skills, close monitoring, and complex care plans.

## Types of Hospitals

Hospitals in the United States are owned by a wide variety of groups and even occasionally owned by individuals. Most hospitals are community hospitals, providing general acute care for a wide variety of diseases. In terms of ownership, three major types of facilities exist:

- *Government hospitals* are owned by federal, state, or local governments. Federal and state institutions tend to have special purposes such as the care of special groups (military, mentally ill) or education (hospitals attached to state universities). Local government includes not only cities and counties but also in several states, hospitals are authorities that have been created from smaller political units. Local government hospitals in large cities are principally for the care of the poor (also referred to as Safety-Net facilities) but many in smaller cities and towns are indistinguishable from not-for-profit institutions. Unfortunately, there are 300 fewer public hospitals today than 15 years ago, with Safety-Net hospitals having closed in Los Angeles, Washington, D.C., St. Louis, and Milwaukee.<sup>5</sup>
- *Not-for-profit hospitals* are owned by corporations established by private (nongovernmental) groups for the common good rather than individual gain. As a result, they are granted broad federal, state, and local tax exemptions. Although they are frequently operated by organizations that have religious ties, secular (or nonreligious) not-for-profit hospitals constitute the largest single group of community hospitals both in number and in total volume of care, exceeding religious not-for-profit, government, and for-profit hospitals by a wide margin.
- *For-profit hospitals* are owned by private corporations, which are allowed to declare dividends or otherwise distribute profits to individuals. They pay taxes like private corporations. These hospitals are also called investor owned. They are usually community hospitals, although there has been rapid growth in private psychiatric and other specialty hospitals. Historically, the owners were doctors and other individuals, but large-scale publicly held corporations now own most for-profit hospitals. These



facilities have had different periods of growth but have never accounted for more than 15% of all hospitals.<sup>6</sup> Except for having the obvious right to distribute dividends and the obligation to pay taxes, for-profit owners function similarly as not-for-profit owners.

Most of the US hospitals are small but larger hospitals provide the majority of the services.<sup>7</sup> The merger of hospitals has reduced the space requirements on a per-bed basis. This reduction in space is most noticeable in facility support services and patient/visitor intake and processing space. This reduced need for inpatient space is often lost, however, on the expanding need for outpatient facilities. The cost to convert inpatient bed space is often too costly to convert to outpatient services, and thus the space is often left vacant depending on the age and condition of the structure.

In addition to the ownership of hospitals, the type of medical specialty is another way to differentiate facilities. Basic medical specialties include pediatric, medical/surgical, rehabilitative, long-term care, and psychiatric facilities. The teaching hospital generally has elements of these specialties in addition to research, education, and clinic activities. Each of these specialty-care facilities presents unique security and safety challenges, which will be explored throughout this text.

The critical access hospital program, created by federal law in 1997, was designed to slow the closing of small rural hospitals. To be awarded the designation as a critical access hospital, the organization must have no more than 25 beds and must be the sole health-care facility within a 35-mile drive. Critical access hospitals enjoy a financial advantage over other hospitals in that they are reimbursed by Medicare on a cost-plus basis instead of at a flat fee by procedure. This financial advantage has allowed many small rural hospitals to remain open and viable.

## Nonhospital Side of Healthcare

The traditional healthcare campus has expanded its service boundaries. Physician offices, outpatient surgical centers, home healthcare, and outpatient mental health clinics expand the horizon of healthcare and the role of the security department, on and off campus. These include public clinics, nursing homes, pharmacies, dental clinics, specialty-care facilities, home care programs, hearing centers, hospices, and durable medical equipment suppliers. Many of these are affiliated with general hospitals and clinics but may also operate as independent entities.

These care organizations have become important industries themselves, while remaining a relatively small part of the total expenditure for healthcare.

A reason for the recent expansion and success of these programs can be attributed to the changes in the delivery of healthcare services and patient care patterns, which have stemmed from managed care organizations. With managed care, there is increasing need for case management, which can result in the earlier discharge of patients. Today, it is common for an Emergency Department to assess and triage a patient and determine that the patient is not “sick enough” for hospital admittance and refer him/her to a home

health agency. Ever increasingly, healthcare professionals are traveling into the community to provide services to their customers in the home environment.

## Diverse Stakeholders

The stakeholders in the healthcare environment are numerous and display a vast variety of characteristics. The patient can be a newborn infant, a teenager, a middle ager, or of advanced age—each with unique security concerns and needs. The patient's medical condition and treatment regimen often render the patient less able to take responsibility for his/her own safety and security. The healthcare provider organizations must understand that they have a moral and legal duty to provide a safe and secure healing environment for all patients. This duty is heightened when the patient is less able to provide basic elements of self-protection due to age, dementia and other mental health issues, mobility, and administered medicines.

The healthcare staff range from the highly educated physician and technical caregiver to the food service and grounds staff. A high percentage of caregivers are female, which presents certain protection concerns relative to working late night shifts and often in remote locations.

## Staffing the Medical Care Facility

The delivery of medical care is very labor-intensive, and utilizes a wide range of professional and service staff. The staff-to-patient ratio is extremely high in the pediatric facility and is quite low in nursing homes. The diversity of technical positions continues to increase as new equipment and care procedures develop, yet the need for nurses continues to increase, driving an extraordinary labor demand. Job growth is expected to continue for the healthcare sector well into the future. As a result, the search for qualified workers is becoming increasingly competitive with the shortage of registered nurses, physical and respiratory therapists, radiology technicians, and other positions. The need to replace workers due to retirements and high job turnover are also factors creating the increased labor demand.

The technical specialization of patient care is expected to create a nurse shortage of epidemic proportions as nursing schools cannot keep up with demand. The median age of registered nurses is anticipated to be 50 by 2010 (increasing at a rate of more than twice of all other workforces in the United States), and there are not enough younger workers to replace them. Coupled with the issue that nursing schools are not attracting enough qualified instructors to meet enrollment demand, an imbalance has resulted between the supply of and the demand for qualified workers.

The shortage of registered nurses is already having ill effects on the US healthcare delivery system: 90% of long-term care organizations lack sufficient nurse staffing to provide even the most basic of care; home healthcare agencies are being forced to refuse new admissions; and there are 126,000 nursing positions currently unfilled in hospitals across

the country. As news of the shortage has reached the American public, 81% are aware that there is a shortage, 93% believe that the shortage threatens the quality of care, and 65% view the shortage as a major problem.<sup>8</sup> Further, the current nurse staffing shortage is burgeoning at a time when patient acuity is higher, care more complex, and demand for services often exceeds capacity. Given the anticipated additional demand for healthcare services, it is estimated that by 2020, there will be at least 400,000 fewer nurses available to provide care than will be needed.

The healthcare industry includes establishments ranging from small-town private practices of physicians who employ only one medical assistant to busy inner-city hospitals that provide thousands of diverse jobs, including labs, nursing, various therapies, mental health, etc. Supported by increasing demand and historic profit margins, the healthcare industry is the largest and the fastest growing industry in the United States.

Healthcare firms employ large numbers of workers in professional and service occupations. Together, these two occupational groups account for three out of four jobs in the industry. The role of outsourcing in healthcare depends on the mix of workers needed and varies depending on the size, geographic location, goals, philosophy, funding, organization, and management style of the institution. Employment in healthcare is expected to continue to grow as the number of people in older age groups, with much greater than average healthcare needs, will grow faster than the total population between 2004 and 2014; as a result, the demand for healthcare will increase.

The healthcare industry has begun to focus a great deal of attention on eliminating waste and unproductive work, in turn placing emphasis on implementing best practices and resource efficiency. This has given rise to interest not only in Six Sigma, but also its close cousin, "Lean," which focuses on eliminating waste and other "non-value-added" activity.

Cost containment also is shaping the healthcare industry, as shown by the growing emphasis on providing services on an outpatient, ambulatory basis; limiting unnecessary or low-priority services; and stressing preventive care, which reduces the potential cost of undiagnosed, untreated medical conditions. Enrollment in managed care programs continues to grow. These prepaid plans provide comprehensive coverage to members and control health insurance costs by emphasizing preventive care. Cost effectiveness also is improved with the increased use of integrated delivery systems, which combine two or more segments of the industry to increase efficiency through the streamlining of functions, primarily financial and managerial. These changes will continue to reshape not only the nature of the healthcare workforce, but also the manner in which healthcare is provided.

## Physician Role Impacted

The physician has been severely impacted by managed care and other changes in the healthcare delivery system. The physician specialty has seen less demand and less pay for services. In addition, a tremendous increase has taken place in the number of family practice physicians, often referred to as primary care physicians and gatekeepers for payer groups. The physician solo or partner practices have given way to various group

purchasing power, physician–hospital partnerships, and direct employment by provider organizations. All of these changes have generally resulted in less physician income and control over patient care decisions. In fact, the primary care physician is often monetarily rewarded for limiting the delivery of care.

## The Healthcare Security Administrator

Today's healthcare protection professional is facing an unprecedented strain on security resources and leadership challenges. Changes in the delivery of healthcare services, multiple campus environments, home care, hospice, and community clinics are driving care deeper into the community and off the traditional campus. The closing of mental health facilities (stand-alone and internal hospital departments) requires emergency departments to manage a significant influx of patients with acute and chronic mental health-care problems. Coupled with restrictions promulgated by the Centers for Medicare and Medicaid Services (CMS) that the least restrictive alternative method for restraint and seclusion be used, has been witness to soaring amounts of violence against medical staff and security personnel.

Evolving accreditation standards from the Joint Commission (TJC), the threat of terrorist attacks, correctional care responsibilities, emergency preparedness and the ability to manage patient surge in the event of a disaster, an increase in weapons being brought into healthcare facilities, possible occurrences of infant abductions, and data security requirements of the Health Insurance Portability and Accountability Act (HIPAA) have put more eyes on the effectiveness of healthcare security programs.

The healthcare industry continues to face financial pressures requiring greater security program justification (i.e., performance measurements, return on investments, and development of 3–5-year security master plans). Operating budgets and capital budget requests are under greater scrutiny and require a business-approach-minded security administrator who can think strategically and act tactically. The industry remains people-intensive—over two-thirds (73%) of healthcare security budgets are dedicated to staff resources.<sup>9</sup> This requires individuals who can effectively lead others while leading themselves and the change necessary to increase the levels of protection in the industry.

## The Joint Commission

TJC, through its standards and Elements of Performance (EP), has had the most significant impact of any single element in the improvement of safety and security in America's healthcare facilities over the last 15 years.

TJC was founded in 1951 as the Joint Commission on Accreditation of Hospitals (JCAH), until 1987, when it adopted the name Joint Commission on Accreditation of Healthcare Organizations (JCAHO). In 2007, it introduced a new brand identity with a shortened name—TJC.

TJC is governed by a Board of Commissioners comprising 29 individual members and corporate members that include the American College of Physicians, the American College of Surgeons, the American Hospital Association, the American Medical Association, and the American Dental Association. It should be noted that the Canadian Medical Association was a corporate member when TJC was formed in 1951 and withdrew in 1959 to form their own accrediting organization for Canada.

TJC evaluates and accredits more than 5,000 hospitals and nearly 10,000 other health-care organizations that provide home care, long-term care, behavioral healthcare, laboratory, and ambulatory care services. An independent, not-for-profit organization, TJC is the US's oldest and largest standards-setting and accrediting body in health-care. More recently, TJC has introduced Joint Commission International (JCI) to develop international consultation, accreditation, publications, and education. Together with their affiliate organizations JCI and Joint Commission Resources (JCR), they offer a wide range of products and service offerings to help improve patient safety and quality in healthcare worldwide.

The stated mission of TJC is “to continuously improve the safety and quality of care provided to the public through the provisions of healthcare accreditation and related services that support performance improvement in healthcare organizations.” Currently there are over 18,000 healthcare organizations accredited through TJC process which officially began accreditation in 1953. [Table 1-1](#) lists all of the specific healthcare industries in which TJC has manuals and standards.

The security standards and EP are found in the *Comprehensive Accreditation Manual for Hospitals*, which is a subscription series with quarterly updates. The subject of security is specifically addressed in the chapter entitled Management of the Environment of Care (EC). There are various standards relating directly and indirectly to the security function in other chapters of the Hospital Accreditation Manual as well.

## Design and Implementation

The format of the standards is broken into two categories, referred to as “design” and “implementation.” The first category is concerned with the organization plan for compliance. The plan is developed through the assessment process and the application of organization (or outsourced) resources. The second category is putting the plan into

**Table 1-1** TJC Healthcare Industry Manuals and Standards

TJC Standards Manuals	
<ul style="list-style-type: none"> <li>• Ambulatory Care Settings</li> <li>• Assisted Living</li> <li>• Behavioral Health Care Organizations</li> <li>• Critical Access Hospitals</li> <li>• Home Care</li> <li>• Preferred Provider Organizations</li> </ul>	<ul style="list-style-type: none"> <li>• Hospitals</li> <li>• Laboratory Services</li> <li>• Long-Term Care</li> <li>• Networks</li> <li>• Office-Based Surgery</li> </ul>

action to achieve the compliance goal. Immediately upon implementation, the plan and performance objectives are measured as an ongoing activity in a cycle to constantly improve (or maintain) performance. This cycle, demonstrated in [Figure 1-1](#), can be referred to as the “EC management process.”

## Organization Surveys

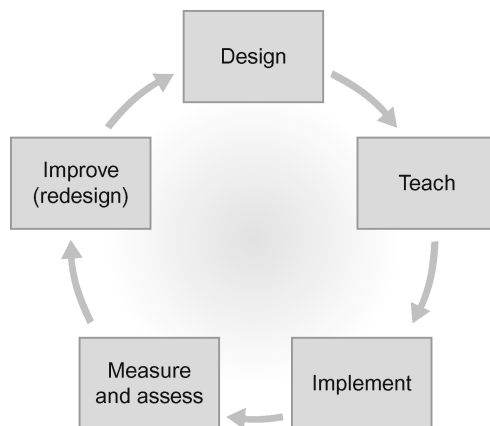
TJC’s approach to accreditation is patient-centered and data-driven. The on-site accreditation process is centered on the Tracer Methodology where surveyors follow the actual experiences of a sample of patients as they interact with their healthcare team, and evaluate the actual provision of care provided to these patients. This review is designed to look at how the individual components of an organization interact to provide safe, high-quality patient care.

An organization seeking accreditation is generally surveyed on a three-year cycle. In 2006, TJC began conducting on-site accreditation surveys and certification reviews on an unannounced basis. Conducting unannounced surveys is believed to provide surveyors the ability to observe and assess healthcare services as they are normally delivered. Random surveys, surveys for cause, and sentinel events can result in a limited review survey.

Denial of accreditation, conditional accreditation, or provisional accreditation can result in various remedial and follow-up actions by TJC.

In July 2007, TJC began conducting on-site validation surveys of a sample of those organizations that are required to submit Evidence of Standards Compliance (ESC). Designed to replace the original random unannounced surveys of all accredited organizations, TJC purports that 5% of accredited organizations will be selected for unannounced on-site ESC evaluations.<sup>10</sup>

The Periodic Performance Review (PPR) is a TJC-designed tool used for self-evaluation of an organization’s compliance with TJC standards. Organizations have the option of



**FIGURE 1-1** Environment of care management process.

asking Joint Commission staff to review that PPR and associated action plans. TJC staff can make suggestions to help the organization improve the quality of care it provides.

When a new standard with an annual reporting or measurement requirement is implemented midyear, it is expected that the requirement be met no later than 1 year from the implementation dates, for example, effective date 7/1/XX, the associated annual requirement would be due by every 6/30/XX.

## Scoring of Standards

In 2004, TJC changed its scoring and accreditation decision process from a score-based system that encouraged organizations to “ramp up” to do well on a survey to achieve a high score to its current accreditation decision process that:

- focuses on ongoing standards compliance.
- is more credible, assuring the public that accredited organizations have demonstrated full compliance with the standards.
- is based primarily on the number of standards that are scored not compliant.
- simplifies the compliance screening process in determining an accreditation decision.
- focuses less on “scores” and more on using the standards to achieve and maintain excellent operational systems.<sup>10</sup>

Compliance with the standards is scored by determining compliance with EP, which are specific performance expectations that must be in place. EP’s are scored on a three-point scale:

- 0 = insufficient compliance
- 1 = partial compliance
- 2 = satisfactory compliance

Each standard has one or more EP. Each EP is labeled in the accreditation manual and all have the same weight. EPs are divided into three scoring categories:

- **“A” EP**—usually relate to structural requirements (e.g., policies or plans that either exist or do not exist such as infant abduction response)
- **“B” EP**—relate to the presence or absence of requirements and are usually answered yes or no. If the organization does not meet the requirements, the EP is scored 0. If there is concern about the quality or comprehensiveness of the effort but the principles of good process design are met, the EP is scored 1. If applicable principles are met, the EP is scored 2.
- **“C” EP**—are frequency-based EPs and are scored based on the number of times an organization does not meet a particular EP.

## The Environment of Care (EOC) Committee

The “EOC” is made up of three basic components: building(s), equipment, and people. A variety of key elements and issues can contribute to creating the way the space feels

and works for residents, families, staff, and others experiencing the healthcare delivery system. For this purpose, a multidisciplinary group within the hospital comes together to form the EOC committee to address all seven elements of the EOC. This should include the most senior security protection administrator at the facility and involve other security department leaders as determined by the committee.

The committee advises hospital staff and reviews changes to the EC standards and intents. New standards, or clarification of standards, are discussed in this committee and may be forwarded onto other committees such as the Executive Council for discussion and feedback. TJC surveyors closely review group communications and dynamics—surveyors are often found analyzing how well this group collaborates and cooperates together on issues facing the environment in which care is provided. In particular, objectives for this committee should involve:

- reducing and controlling environmental hazards and risks.
- preventing accidents and injuries.
- maintaining safe conditions for residents, staff, and others coming to the organization's facilities.
- maintaining an environment that is sensitive to resident needs for comfort, social interaction, and positive distraction.
- maintaining an environment that minimizes unnecessary environmental stresses for residents, staff, and others coming to the organization's facilities.

## The Sentinel Event

Patient safety is at the core of TJC's standards and policies related to sentinel events (any unexpected occurrences involving death or serious physical or psychological injury, or risk thereof). The term "sentinel event" is a very broad term utilized by TJC in relation to their accreditation process, which has been in effect since January 1999. TJC's Sentinel Event Policy calls for every accredited organization to identify, voluntarily report, evaluate, and evoke sentinel event prevention strategies. The policy requires organizations to investigate the root causes of adverse events, implement appropriate strategies to prevent reoccurrence, monitor the effectiveness of these strategies, and advise the affected patients and families of errors or unexpected outcomes and the steps taken to correct them.

The sentinel event not only relates to protection, but also to a wide array of adverse patient outcomes. Such events are called "sentinel" because they signal the need for immediate investigation and response.<sup>11</sup>

There are four primary goals for the TJC sentinel event policy:

- To have a positive impact on the improvement of patient care.
- To focus organization attention on the event to provide an understanding of the underlying cause, and to make changes in systems and procedures to reduce the probability of such an event in the future.



- To increase the general knowledge about sentinel events, their causes, and preventive strategies.
- To maintain the confidence of the public in the commission accreditation process.

There are two basic categories of the sentinel event relative to the investigation and reporting of such incidents. The first is the event which is referred to as “reviewable” by the TJC. The second is an event that is handled internally within the organization. In the latter event, the organization is required to have a policy regarding a review process which meets TJC criteria but the event does not need to be reported to the TJC.

The subsets of sentinel events that are subject to TJC review at the time of occurrence and that are security-related are (1) an event resulting in an unanticipated death or major permanent loss of function, not related to the natural course of the patient’s illness or underlying condition or (2) the event is the one specified by the TJC and the outcome is not death or major permanent loss of function. This second category specifically includes security incidents of infant abduction or discharge to the wrong family, or rape.

The TJC is not very clear regarding its definition of an infant or the distinction of abduction (stranger to stranger versus domestic custody). There is a vast difference in these two categories of infant abduction incidents.

The rape of a patient is a TJC-reviewable sentinel event. The determination of rape is to be based on the organization’s definition, consistent with applicable law and regulation. An allegation of rape is not reviewable under the TJC’s policy. Applicability of the policy is established when a determination is made that a rape has actually occurred.

Reported sentinel events are compiled into a database which currently contains over 3,200 cases. This vast knowledge base of adverse outcomes helps inform and improve TJC’s standards and policies, and provides “lessons learned” information to healthcare organizations to support their safety improvement efforts. As noted in [Figure 1-2](#), the number of sentinel events has increased dramatically since 1995.

The terms “sentinel event” and “medical error” are not synonymous; events are called “sentinel” because they signal the need for immediate investigation and response. For the healthcare security administrator, examples of reviewable and nonreviewable sentinel events under TJC’s Sentinel Event Policy include assaults, rape, homicide, elopement, restraint deaths, and suicide.<sup>13</sup> [Figure 1-3](#) shows the number of reported assaults, rape, and homicide by year since 1995.

The TJC encourages accredited organizations to report all reviewable sentinel events. The TJC may also become aware of a reviewable sentinel event through patient contact, family, media, or a staff member. Regardless of how the TJC is made aware of the event, the organization is expected to prepare a root cause analysis report and action plan within 45 calendar days of the event or of becoming aware of the event. The analysis and action plans are then to be forwarded to the TJC. Upon receipt of the information, the TJC will determine the acceptability of the analysis and action plan.

An organization that does not submit an acceptable analysis or action plan within the 45-day period may be put on Accreditation Watch. This designation is considered to

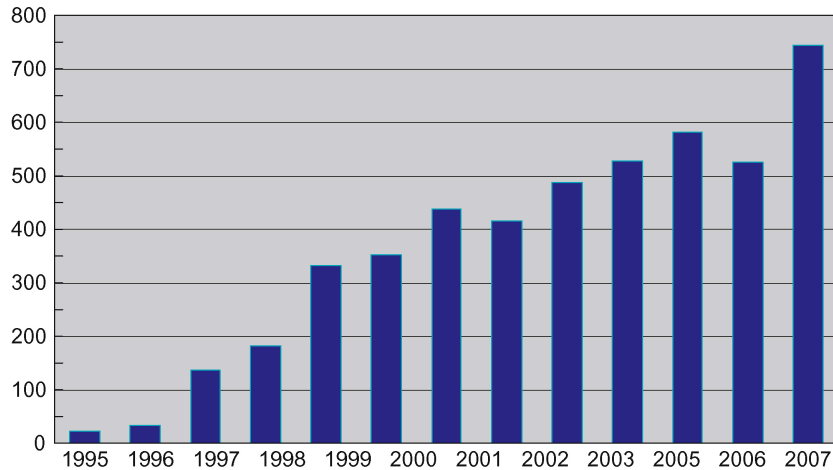


FIGURE 1-2 Total sentinel events reviewed by year.<sup>12</sup>

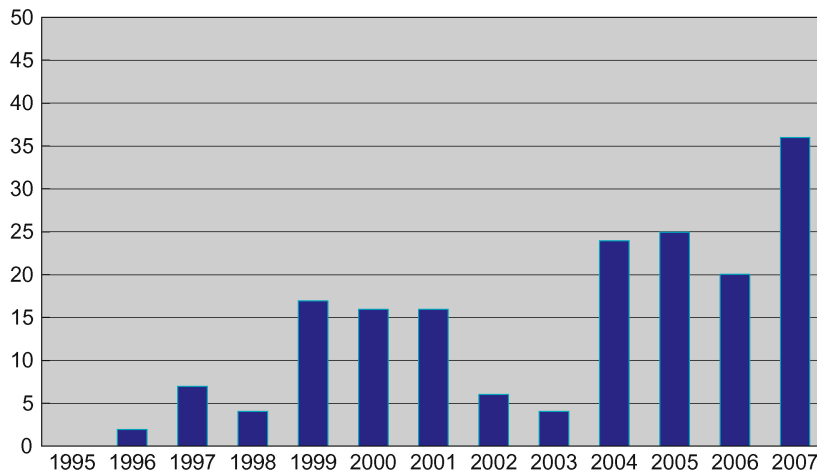


FIGURE 1-3 Sentinel events by year—assault, rape, homicide.<sup>14</sup>

be public information. The Accreditation Watch is not an accreditation status; rather, it is an attribute of the organization's official accreditation.

The removal of an Accreditation Watch is a determination of the TJC's Accreditation Committee. The decision to remove this accreditation attribute generates an Official Accreditation Decision Report. This report will assign an appropriate follow-up activity for the facility, typically a written progress report or follow-up visit to be conducted within a specified period of time.

Until a sufficient period of time passes, there will be various questions and concerns on what is a reviewable sentinel event. As situations occur and questions get answered, the picture will be much clearer than it is today. The best course of action is to have a

strong in-house program to process all sentinel events, and when in doubt as to a mandated reviewable event, to err on the side of reporting it to the TJC.

## Health Insurance Portability and Accountability Act (HIPAA)

This federal law was enacted in 1996 under the direction and control of the Department of Health and Human Services (HHS). The law applies to health information, often referred to as Personal Health Information (PHI), created or maintained by healthcare providers who engage in certain electronic transactions, health plans, and healthcare clearinghouses. The Office of Civil Rights (OCR) is the departmental component responsible for implementing and enforcing the privacy regulation. The agency issued a final Privacy Rule that became effective in April 2001 and became enforceable for most covered entities in April 2005. Regulations are designed to safeguard PHI that is maintained or transmitted in electronic form. Computers, magnetic tape, digital memory cards, the Internet, and extranets are examples of electronic media that may contain PHI.

There is a distinction between the HIPAA terms Privacy Rule (PR) and Security Rule (SR). The PR basically defines what data must be protected, regardless of format, and how they can and cannot be utilized by the organization maintaining and responsible for controlling the data. The SR provides requirements for protecting the defined PHI. It is fairly obvious that HIPAA compliance in the healthcare environment involves several disciplines which include security, risk management, and information technology. It truly requires a multiple disciplinary management approach for implementing compliance policy and procedures.

The term “convergence,” meaning an organized and coordinated effort of security and information technology, is truly at play in managing HIPAA requirements in addition to other major areas of managing security risks. The security function of the healthcare organization will be charged with and responsible for the physical protection of the data and in the area of law enforcement disclosures. It is not uncommon to receive requests for information from law enforcement officials who are unaware that their requests violate either HIPAA or other laws or confidentiality protocols. An example of such a situation occurred in Wisconsin where a nurse was prosecuted for refusing to release information to law enforcement citing the rules of HIPAA. The nurse was charged with obstructing an officer and contempt of court for refusing to allow an officer to serve a patient with a restraining order.<sup>15</sup> It would appear that there was no request by law enforcement for PHI and that simply acknowledging that the patient was in the facility at a specific location would not have violated the HIPAA SR.

A panel reviewing the Virginia Tech massacre noted that federal privacy laws, notably Family Educational Rights and Privacy Act (FERPA), blocked critical stakeholders from sharing information with regard to the mental health of the student who became the shooter. Experts say privacy laws should not stop stakeholders from sharing information and getting intelligence they need to assess a threat. When a person is labeled a harm to himself/herself or others, privacy laws become meaningless. Persons holding confidential

information proving that someone plots violence have a duty to warn the public. Public safety should override the person's civil liberties.<sup>16</sup>

## The Centers for Medicare and Medicaid Services (CMS)

The Medicare and Medicaid programs were signed into law in 1965. There have been various changes in the law since that time when the basic CMS programs were part of Social Security. CMS was known previously as the Health Care Financing Administration. CMS is responsible to administer Medicare, Medicaid, and Child Health Insurance Programs.

The stated mission of CMS is to ensure effective, up-to-date healthcare coverage and to promote quality care for beneficiaries. A principal element of the CMS provider reimbursement program for rendering medical care is to “approve” the provider. Upon this approval the provider must formally agree to the CMS Conditions of Participation (CoP) to be eligible for payment of services rendered.

In relation to hospitals, CMS relies on several accreditation programs to inspect (survey) patient care practices in terms of meeting quality control standards. Currently there are three CMS-approved accreditation programs, which are:

- TJC
- American Osteopathic Association (AOA)
- Det Norske Veritas Healthcare, Inc. (DNV)

The DNV program is called the National Integrated Accreditation for Healthcare Organization. Its program integrates with the International Organization for Standards' ISO-9001 quality management system standards and with the Medicare conditions of participation. The DNV approval is the most recent, being conferred in the fall of 2008.

In addition to making healthcare payments to providers and the states on behalf of beneficiaries, CMS provides Survey and Certification programs to ensure that providers and suppliers comply with Federal health, safety, and program standards. These are administered per agreements with state survey agencies to conduct on-site facility inspections. TJC is recognized by the CMS as an equivalent substitute for its own inspections but a facility is not immune to a CMS inspection in the days or weeks following a TJC survey.

CMS utilizes regulation and enforcement activities to help meet its vision of “the right care for every person every time” that affects all aspects of the US healthcare delivery system—hospitals, nursing homes, laboratories, and home care. Applicable standards are set that affect the healthcare security administrator in the area of security's involvement in patient care—elopement (prevention and response), restraint and seclusion, and use of weapons. The reduction in the use of physical restraints has been one of CMS's major quality initiatives.

In December 2006, CMS issued guidance on HIPAA security with regard to remote use of and access to electronic protected health information (EPHI). This guidance reinforced the obligations of covered entities to comply with the SR and provided specific

guidance for protecting EPHI when it is accessed or used outside of the covered entity's physical purview or location. While these issues are encompassed by the general standards contained in the SR, they are not explicitly addressed.<sup>17</sup>

With regard to HIPAA enforcement activities (nonprivacy), the CMS continues to operate based on a complaint-driven process, addressing complaints filed against covered entities by requesting and reviewing documentation of their compliance status and/or corrective actions.

## References

1. Alonso-Zaldivar, R. (2008, January 1). Health care a \$2 trillion issue for '08 campaign. *Denver Post*. Available at [http://www.denverpost.com/ci\\_7906958?IADID=Search-www.denverpost.com](http://www.denverpost.com/ci_7906958?IADID=Search-www.denverpost.com). Accessed on January 2, 2008.
2. U.S. Department of Health and Human Services. (2007, November). CMS financial report (fiscal year 2007). Available at [http://www.cms.hhs.gov/CFOReport/Downloads/2007\\_CMS\\_Financial\\_Report.pdf](http://www.cms.hhs.gov/CFOReport/Downloads/2007_CMS_Financial_Report.pdf). Retrieved on July 8, 2008.
3. Alonso-Zaldivar, R. (2008, January 1). Health care a \$2 trillion issue for '08 campaign. *Denver Post*. Available at [http://www.denverpost.com/ci\\_7906958?IADID=Search-www.denverpost.com](http://www.denverpost.com/ci_7906958?IADID=Search-www.denverpost.com). Retrieved on January 2, 2008.
4. Pho, K. (2008, April 23). Wasted medical dollars. *USA Today*. Available at <http://blogs.usatoday.com/oped/2008/04/wasted-medical.html>. Retrieved on June 13, 2009.
5. Dewan, S., & Sack, K. (2008, January 8). A safety-net hospital falls into financial crisis. *The New York Times*. Available at <http://www.nytimes.com/2008/01/08/us/08grady.html>. Retrieved on June 13, 2009.
6. Griffith, J. R., & White, K. R. (2006). *The well-managed healthcare organization (6th ed.)*. Chicago: Health Administration Press.
7. American Hospital Association. (2007). 2007 Chartbook: trends affecting hospitals and health systems. Available at <http://www.aha.org/aha/research-and-trends/chartbook/2007chartbook.html>. Retrieved on November 9, 2008.
8. The Joint Commission. (2009, June 29). Health care at the crossroads: strategies for addressing the evolving nursing crisis. Available at [http://www.jointcommission.org/NR/rdonlyres/5C138711-ED76-4D6F-909F-B06E0309F36D/0/health\\_care\\_at\\_the\\_crossroads.pdf](http://www.jointcommission.org/NR/rdonlyres/5C138711-ED76-4D6F-909F-B06E0309F36D/0/health_care_at_the_crossroads.pdf). Retrieved on July 8, 2009.
9. Weonik, R. (2008, January 21). Securing our hospitals: GE Security and IAHS healthcare benchmarking study. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
10. The Joint Commission. (2008). Evidence of standards compliance validation surveys and random unannounced surveys. Available at <http://www.jointcommission.org/AccreditationPrograms/Hospitals/AccreditationProcess/scoring>. Retrieved on July 13, 2008.
11. Joint Commission Resources. (November/December 1998). *Special Report on Sentinel Events, Perspectives* (pp. 19–42). Oakbrook Terrace, Illinois.
12. The Joint Commission. (2008). Sentinel event statistics. Available at <http://www.jointcommission.org/SentinelEvents/Statistics/>. Retrieved on December 31, 2008.

13. The Joint Commission. (2008). Sentinel event policy and procedures. Available at <http://www.jointcommission.org/SentinelEvents/PolicyandProcedure/>. Retrieved on December 31, 2008.
14. The Joint Commission. (2008). Sentinel event statistics. Available at <http://www.jointcommission.org/SentinelEvents/Statistics/>. Retrieved on December 31, 2008.
15. Tomes, J. P. (2005). Prescription for data protection. *Security Management*, 78(April).
16. Harwood, M. (2008, April). Teaming up to reduce risk. *Security Management*. Available at <http://www.securitymanagement.com/article/teaming-reduce-risk>. Retrieved on June 13, 2009.
17. U.S. Department of Health and Human Services. (2007, November). CMS financial report (fiscal year 2007). Available at [http://www.cms.hhs.gov/CFOReport/Downloads/2007\\_CMS\\_Financial\\_Report.pdf](http://www.cms.hhs.gov/CFOReport/Downloads/2007_CMS_Financial_Report.pdf). Retrieved on July 8, 2008.

# Protecting a Healing Environment

The healing environment presents a host of different and unique settings where patient care is the primary mission. These traditional environments include hospitals, clinics, physician and dental offices, neighborhood emergency care centers, home care rehabilitation, long-term care, and free-standing surgery centers—each presenting equally unique needs for protection of patients, staff, visitors, contractors, and property.

There are also healing environments that often escape the more standard patient care environments such as veterinary hospitals, clinical trials, clinics, and blood banks. The Red Bank Veterinary Hospital in Tinton Falls, NJ, is an example of a large healing environment. This facility provides numerous specialties such as cardiology, dentistry and oral surgery, dermatology, internal medicine, neurology, oncology, ophthalmology, and surgery. The facility is the largest privately owned veterinary hospital in the United States. The hospital employs over 300 staff providing services in 58,000 square feet of space, which includes 25 exam rooms, surgical suites, and 120-seat lecture hall for continuing education programs.<sup>1</sup>

In the last decade progress in providing safe and secure healthcare environments has “paled” in contrast to other major business segments of our society. While the tragic events of the World Trade Center on September 11, 2001 jump started improved security for most US organizations, the event had little overall effect on improving healthcare security. Since 9/11 serious crimes such as homicides and serious assaults have steadily increased in virtually all healthcare environments.

## Defining Healthcare Security

The term *security* or *protection for healthcare facilities* can often be vague and elusive. It is in fact a relatively ill-defined concept that can and does take on different connotations in different settings. In the context of protecting healthcare facilities, security can be generally defined as a system of safeguards designed to protect the physical property and to achieve relative safety for all people interacting within the organization and its environment.

This definition, of course, leaves the problem of defining *relative safety*. What is safe today may not be safe tomorrow. It is a difficult task to evaluate the environment of a particular facility to determine if relative safety has in fact been achieved and such evaluations are somewhat subjective in nature. The realistic goal of protection, or security,

is intended to reduce the probability of detrimental incidents and mitigate incident damage, not to necessarily eliminate all such risks. Security, then, is not static and can be viewed as a state or condition that fluctuates within a continuum. As environmental and human conditions change, so does the status or level of protection. It is this phenomenon that requires organizations to constantly evaluate and re-evaluate their system of protection on a continuous basis.

In some cases, healthcare security practitioners tend to view security too strictly or too definitively. The organization being served is the entity that provides the ultimate definition of the security system; after all, the organization provides the funding. This is not to say that the protection program and the philosophy and objectives of the principal security administrator do not have a strong influence on molding the organizational definition.

A common error for healthcare organizations is to view security as being closely aligned with the law enforcement function. Although some common ground may exist between security and law enforcement, at least 90% of their respective activities are different. Security of the healthcare organization must be viewed as a business function specific to that organization while law enforcement may be viewed as external protection that attempts to uphold the law for all of the society. Having said that, law enforcement and even the military have the overall goal of providing a “state of security.” [Table 2-1](#) portrays the general differences between law enforcement and security.

An extremely important concept of guiding the healthcare security system is that of “administrative remedy” versus “law enforcement remedy.” The goal of the administrative remedy is to resolve a situation in the best interests of the organization, possibly negating the need of a law enforcement approach when facts and circumstances indicate that there may be a better organization-based resolution. These circumstances might include petty theft where restitution and disciplining action or a substance abuse issue may best be resolved via employee/physician assistance programs. The administrative remedy concept does not in any way imply that criminal information should not be reported to the police. Law enforcement agencies and prosecution in virtually all jurisdictions must set priorities consistent with the resources available. The result is that minor crimes can

**Table 2-1** Comparing Basic Characteristics of Law Enforcement and Security

Security	Law Enforcement
Prevention of Incidents	Apprehension of Offenders
Protecting an Organization	Protecting a Society
Administrative Remedies	Legal Remedies
Organization Defined	Statute Defined
Private and Tax Funding	Tax Supported
Return on Investment	Public Opinion

*NOTE: Some law enforcement agencies are supported by quasi private funding such as the Public Safety Department of various colleges and universities.*



often be ignored or lost in the process. Once an organization “hands off” a situation to law enforcement, it is often more difficult to then attempt to affect an organizational remedy.

## Basic Rationale of Healthcare Security

There are a multitude of reasons mandating the provision of the proper level of security and safety for the healthcare environment. These reasons include a moral responsibility, legal concerns, complying with accreditation/regulatory requirements, contributing to the provision of quality patient care, maintaining the economic/business foundation of the organization, and maintaining sound public, community, and staff relations.

In terms of a moral responsibility, the organization has an obligation to manage its environment for “the good” that minimizes the possibility of injury or death to all persons on its premises. This moral responsibility extends to reasonable steps to preclude the destruction, misuse, or theft of property. A second justification for providing protection services is a legal responsibility. The healthcare organization has a duty to exercise care and skill in the day-to-day management of corporate affairs. The healthcare organization’s obligation to its patients is contractual in that the organization assumes certain responsibilities toward them.

The issue of liability in the management of patient medical services and care facilities has become more acute in recent years. An organization may be held liable for the negligence of an individual employee under the doctrine of “respondent superior” or for corporate negligence. In terms of employee negligence, two general factors are requisite for imposing liability on the corporation. An employer–employee relationship must exist, and the employee’s act or failure to act must occur within the scope of his or her employment. Corporate negligence occurs when the organization maintains its building and grounds in a negligent fashion, furnishes defective supplies or equipment, hires incompetent employees, or in some other manner fails to meet accepted standards, and such failure results in harm or injury to a person to whom the organization owes a duty.

One aspect of the legal rationale is the growing element of punitive damages. Jury awards that punish organizations for not taking appropriate security measures continue to increase in frequency and in higher awards. In many jurisdictions punitive damage awards are not covered by insurance and must be paid from the organization’s funds.

A third important reason for maintaining a safe and secure environment is the responsibility of complying with accreditation, licensing, as well as federal, state, and local regulatory agencies. Failure to meet such compliance requirements can seriously undermine the success and viability of the organization.

A fourth rationale for providing a protection system is to maintain a sound economic foundation for the organization. In this regard, healthcare has faced mounting criticism, especially in regard to the rapidly escalating costs of delivering quality medical care. Critics often cite the lack of cost-containment measures that, in part, relate to preventing theft and the waste of supplies and equipment. It is estimated that between 3% and 10% of hospital expenditures could be saved if proper security controls were implemented.

Yet in most cases, the entire protection budget for healthcare facilities is generally less than 1% of the total operating budget with the majority of the security budget directed to personal safety issues.

Last, a safe and secure environment is required to maintain good public and employee relations. Although this reason does not appear to be as important as the others, it has probably been responsible for providing more funds for the security budget than the other four justifications combined. Healthcare administrators who face bad media coverage relative to a security problem or restless employees threatening to walk out over a security incident somehow find new funds to make positive adjustments in the protection program.

## Evolution of Healthcare Security

The evolution of *healthcare* security is based on *hospital* security. A large part of hospital security's heritage can be found in the history of Great Britain. History reveals that one of the first traces of an organized hospital in the United Kingdom was the Smithfield in London, founded in 1123. The hospital was granted a Royal Charter by King Henry VIII in 1546. In 1552, the House of Governors authorized the implementation of "the Order of the Hospital," what are now known as position or job descriptions. The Office of the Porter was responsible for the beadles or the stationed guards. This marks the beginning of healthcare security as we know it today.

Until 1948, hospitals in the United Kingdom operated under boards of governors. In 1948, the Department of Health and Social Security was created, and the Social Services Act went into effect. At this time hospitals in major cities employed a security officer known as a *house detective*. In the late 1950s and early 1960s the position title was changed to *security advisor*.

During the early 1970s, hospitals made a concerted effort to create a more efficient protection system and now have very good protection programs in place. The authors gratefully acknowledge John E. Nichols, former District Security Officer of the British Health Service and author of *Guide to Hospital Security* (Gower Publishing Co. Ltd., Aldershot, Hampshire, England, 1983), for this information.

## Progression of Hospital Security in the United States

To understand better the current status of healthcare security, a review of how hospital security has evolved over the last 100 plus years in the United States will provide a basic perspective. For purposes of discussion, this history has been divided into six periods, each of which reflects a somewhat different philosophy or overall approach to the concept of hospital security.

### 1900–1950

During this time period little mention was made of the term *security* in relation to protecting the hospital. Initially, the basic protection activities were performed entirely by

maintenance workers as they completed their physical plan duties. As facilities grew in size, some hospitals hired a guard to conduct facility rounds to relieve the maintenance person of this task. The primary emphasis of the guard's rounds was the fire watch. Maintaining the physical plant, including the fire watch, was the primary responsibility of the engineering/maintenance function.

#### *1950–1960*

Around 1950 protection was expanded to include various aspects of law enforcement. The fire watch continued to be an important protection function; however, the fire watch and law enforcement operated independently of each other. It was during this time that there was an abundance of police officers in many of the larger police departments; however, criminal activities were beginning to be noticed in and around hospitals. It became fairly common for larger police departments to station a police officer at a hospital or at least to use a hospital as the hub of the neighborhood beat. The police presence at hospitals came at taxpayers' expense, but at this time the nation's hospitals were viewed as public and community institutions. As the need for more protection became apparent, hospitals naturally hired off-duty policemen to provide additional security. The shift from the beat officer to vehicle patrols basically eliminated city-funded coverage for most hospitals.

#### *1960–1975*

Beginning around 1960, hospitals became aware that protection of the organization was not limited to just fire hazards and criminal activities. Security was perceived as a specialized management service touching all departments and functions of the healthcare organization. The idea of security as a management service created the need to review the organizational reporting level of the protection function. The result was the creation of a security department that reported to an administrative-level position. In many cases the security department reporting level was to the Director of Maintenance and Engineering. The use of off-duty police officers declined during this period and security departments began staffing with in-house personnel as a general rule.

#### *1975–1990*

The management services concept continued to prevail during this period, but the definition and day-to-day functions of security continued to expand. The most noticeable activity in this regard was in the area of safety. Many security departments became so involved in safety that they were renamed *Security and Safety*. The department director became more involved as a member of the top management team. During this period the mission of the security department changed from being primarily a reactive function to a proactive (prevention) type of program, and the use of off-duty police officers continued to decline while the utilization of contract security officers began to increase.

#### *1990–2000*

In the early 1990s rapid change began to take place. The concept of risk management, introduced in the 1980s, was now maturing and bringing a new appreciation for the protection

effort. Security departments were expanding their service roles while at the same time facing severe budget constraints. They were being asked to do more with less. There also developed a great diversity of security programs with a general trend to break away from security resulting in two complementary but separate programs. Some security departments were downsizing in terms of staffing, function, and budget, while other programs were growing. The growing programs simply had a broader view of security and the interrelationship of other hospital functions to the protection program. In these programs the security department often took up the slack of providing a broader range of services due to the downsizing of other hospital support programs. A good example of the movement is the merging of security and hospital telecommunications into a single department. Another area of consolidation can be found in the merging of transportation services and security into a new and expanded department. Moving into the new century, the utilization of outsourced services continued to replace proprietary security departments in addition to outsourcing other hospital support departments such as food services, environmental services, biomedical engineering, and laundry services.

### *2000–2009*

The introduction of new and expanded technology provided a very positive impact on security programs. At the same time it introduced a host of new and changing security risks. The integration of physical security elements of protection and the concept of convergence reshaped the working interrelationship of security and information technology. Convergence led to the concept of enterprise management which continues to develop and will continue to be a major linkage in protecting the healthcare environment.

The mission and goals of security and safety became more distinct and separate as both disciplines continued to grow and mature. This distinction of roles and the growing importance of each have apparently escaped the comprehension of The Joint Commission (TJC). In 2009, TJC combined safety and security standards into a single element of the Environment of Care.

The working relationship and the need for greater coordination and support between security and emergency management became quite clear in this 10-year time period. The events of 9/11 and Hurricane Katrina each demonstrated important lessons for hospitals about organizational response and overall preparation for mass casualty events and the associated security risks. These coordinated efforts will continue to expand in the years ahead and it is highly likely that the role of emergency management will be merged into the security department as a major component of the overall facility security program.

During this period there has been an unprecedented move to the over-utilization of security staff in providing certain aspects of patient care. This over-utilization occurs primarily in the emergency department due in large part to the reduction of funding and subsequent lack of medical care resources for the treatment of mental health patients. This increased security role in supporting patient treatment issues has occurred without an increase of security personnel. The result has been an increase of security-related incidents

**Table 2-2** Summary of Changing Characteristics of US Healthcare Security by Time Period

Period	Basic Changes/Characteristics of Healthcare Security
1900–1950	Primary duty was a fire watch as a function of maintenance and engineering.
1950–1960	A general law enforcement approach evolved.
1960–1975	The development of in-house security departments with expanded duties and responsibilities.
1975–1990	The security function was viewed as an integral part of management and the function became a valued component of the patient care team. Outsourcing of security increased.
1990–2000	Security continued to expand services while at the same time safety was generally separated into its own department. As risk management developed, security took on a greater role in prevention of incidents and improving emergency response capabilities, somewhat in response to reduced police resources/response.
2000–2009	Increased crime, terrorism concerns, and organization demand for increased security services prevailed. New technology both aided security and created new and often complicated security risks. Increased violence and lack of mental health care resources created increased security support of patient care issues, downgrading overall protection levels.

and degradation of the general level of protection for many healthcare facilities as a whole. [Table 2-2](#) provides a summary of the changing characteristics of US healthcare security by time period.

## Security, Risk Management, Safety

The security program is not a single stand-alone function that provides total protection for the healthcare organization. Virtually all departments and functions within the organization are expected to, and do, contribute to the overall level of facility safety and security. The safety function and the risk management function are two primary contributors to the protection system. Security must interact with these functions on a day-to-day basis providing a coordinated and supportive approach to the common goal of maintaining a safe environment.

### Safety Services

The equipment, processes, and procedures used to cure illness and mend injuries combine to create an environment requiring a high level of safety programming. There is an interrelationship between security and safety in that the goal of each is to prevent human suffering and avoid costs to the organization. Safety deals primarily with acts and conditions where there is generally no conscious rationale to do harm. On the other hand, the primary business of security deals with acts where there is a conscious decision or rationale

to do harm. An example is fire. Safety is basically concerned with the accidental fire while security would be more directly concerned with the arson aspect of the fire. Both security and safety play an important role in the prevention of fire regardless of the cause. Security is expected to directly support the safety effort through accident investigations, hazard reporting, and the correction and/or reporting of unsafe acts.

The prevention of accidents is a primary objective of the safety efforts that requires identifying safety risks. While inspections are intended to identify risks, a good accident reporting system will supplement the inspection process.

Patient accident reporting is generally the responsibility of the caregiver as it clearly falls into the realm of patient care. Only in rare circumstances would security be called upon to conduct an investigation or to file a report in these cases. Examples of the need for security involvement would, however, include a suicide, attempted suicide, disappearance of a patient, a fire, and when a patient accident occurs in a public area of a facility.

The investigation and reporting of staff accidents are generally the responsibility of the department of supervision. Security would become involved if the accident was severe and emergency response was required.

The reporting and investigation of visitor accidents is frequently neglected, despite the fact that the visitors are the source of many litigation proceedings against health-care facilities. The basic problem appears to be that the responsibility for reporting visitor incidents is not as clearly defined as staff and patient accident reporting policies and procedures. Because it is everyone's responsibility, it is sometimes not accomplished. The investigation of all visitor accidents should be a security function responsibility.

## Risk Management

The term *risk management* is relatively new compared with the term *security* at least in the healthcare environment. Healthcare risk managers are a group of staff support personnel for healthcare provider organizations. Their role developed less than 25 years ago as medical malpractice claims became a major concern. The goal of risk management in the healthcare setting is to prevent patient injury and prevent or limit financial loss to the healthcare organization. Risk managers often spend a great deal of time dealing with contracts, equipment technology, insurance administration, and problems involving potential or actual liability. It is thus not surprising to find that many risk managers have a background in law and/or clinical experience.

### *Components of Risk Management*

Although it varies from organization to organization, a written statement of function, authority, and responsibility is absolutely essential to the effective functioning of a risk management program. The security effort should be considered an element of total organization risk management; however, security rarely reports to risk management. As shown in [Figure 2-1](#), numerous elements can be integrated into a coordinated program.

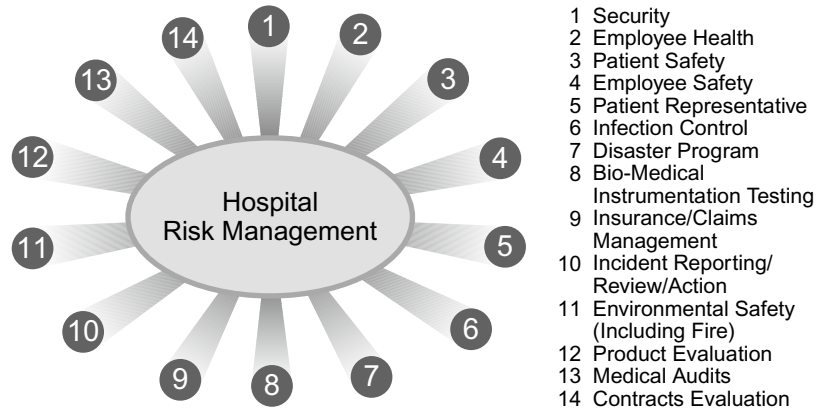


FIGURE 2-1 Typical components of risk management.

## Developing the Security System

A healthcare security system is developed by applying security safeguards to manage the security vulnerability and risks identified by the organization. A safeguard is simply an element or component of the protection system. Safeguards can be viewed in two basic categories of physical safeguards and psychological safeguards.

Although one can differentiate between psychological and physical control, most physical controls also provide an element of psychological protection. A good example is night lighting. Because a parking lot is well lit does not mean that it is more difficult to commit a crime there than in a poorly lighted lot. The lighting itself is a physical control, and also functions as a psychological deterrent. The television camera or monitor cannot reach out to stop an incident or to catch a wrongdoer. It serves as a psychological deterrent, since wrongdoers, or potential wrongdoers, probably do not know the extent of the system. They might wonder who may be watching, what resources may be deployed, and whether a video recording is translating the images into evidence. [Table 2-3](#) lists some of the more common security safeguards.

## Psychological Deterrents

Realizing that physical controls cannot protect all things in all places, professionals also use psychological deterrents, which are directed at the decision-making process of the individual. For the purposes of security planning, a psychological deterrent is defined as an individual's interpretation of a situation in which the potential positive or negative aspects of behavior serve to prevent or preclude the expression of that behavior.

The fundamentals of Crime Prevention through Environmental Design (CPTED) follow these principles as they include using the physical environment and other aspects of design to manage behavior. The proper design and effective use of the built environment

**Table 2-3** Common Psychological and Physical Security Safeguards

Psychological	Physical
Signage	Security Officers
Visitor Badging/Sign-In Logs	Alarms
Marking/Labeling	Closed-Circuit Television
Aggressive Incident Investigation	Glazing
Policy of Prosecution	Barriers
Conditions of Employment	Lighting
Enforced Disciplinary System	Safe/Containers
Greetings/Staff Acknowledgment	Access Controls
Way Finding and Guidance	Identification Badges
Landscape Design/Architecture	Emergency Communication Devices

can lead to reduction in the incidence of and fear of crime as well as affect the behavior of people by providing physiological and psychological deterrence.

## Factors in Motivation

When people act in any way, good or bad, it is because they are motivated to act. Behavior is observed as a contemporary event—a dynamic relation between the organism and its environment. Motives, on the other hand, are not directly observable in the sense that actions and even emotions, learning, memory, and intelligence are observable; rather, motives are inferred or hypothesized from behavior.

### *Age*

In a study conducted by researcher Alice Peckett Franklin, 12% of the work force at a retail outlet was between the ages of 18 and 22. This group was associated with 69% of the reported thefts. One explanation for this phenomenon, offered by Richard C. Hollinger and John P. Clark in *Employee Theft*, is that younger workers do not feel as committed to an employer as senior workers do. Older workers risk losing their vacation, sick time, retirement benefits, and longevity pay, which younger workers have not yet achieved.<sup>2</sup>

### *Society and Motives*

Motives that involve other people, either directly or indirectly, are called social motives. They are distinguishable from psychological drives because their form is usually determined by the individual's culture through rules, regulation, and taboos. Human behavior must fit into the pattern of activity that society dictates or the individual risks rejection by society.



Most people resist some of their tendencies toward antisocial behavior, not because of moral qualms but because of their fear of the consequences. The inhibition of antisocial tendencies is acquired in the course of individual development, and this depends on the moral code and convention of the given culture.

Differences in motivation often account for the fact that different people may react differently when confronted by the same set of circumstances, and one person may behave differently when confronted by a particular set of circumstances on different occasions. This variability presents a challenge to the healthcare security practitioner.

### *Conscious Versus Unconscious Motivation*

Only a very small part of an individual's knowledge can be in consciousness at any given moment. The belief that humans are rational animals who make their plans with foresight is appealing, but it is an incomplete statement of human nature. Analytical experience of psychologists demonstrates that the conscious self-restraint of instincts plays only a modest role compared with such emotional factors as the desire for love or the fear of punishment. Actions are determined more by unconscious than by conscious motivation.

There is, however, a constant interplay between the conscious and the unconscious mind. The unconscious mind contains knowledge accumulated in various ways throughout life. The vast storehouse contains past experiences of finding gratification for needs, the consequences of these past efforts, and the feelings that are aroused. As the environment changes and new possibilities are offered for gratification, the memories of past experiences that are most similar and pertinent to the current external conditions are recalled.

The unconscious mind, the reservoir of total memory and intuitive judgment, is the part most influenced by suggestion and imagination. A suggestion that seems to strengthen ideas already present usually produces action. In this regard, a strong and viable protection system will strengthen the individual's inclination to maintain acceptable social behavior.

Security preventive programming is concerned primarily with one area of motivation: directing behavior through the fear of being caught and the possibility of being punished. It has long been recognized that fear strongly motivates human behavior, and the threat of punishment has a retarding effect on individual impulses. Parents use fear to direct the conduct of their children. School, church, and state institutions also use fear to produce a desired form of behavior, when necessary. This is not to imply that fear is the only reason people refrain from negative behavior. Other motives, including perceived needs; conscience; conditions like fatigue, illness, or anxiety; past experiences; and personal goals, play an important part in determining this behavior.

### *External Motivation*

In *The Organization Man*, William Whyte describes how significantly humans have changed over the years. Several decades ago they were "inner-directed," but today they have become "outer-directed." By this Whyte means that individuals get their "motivation orders" from outside.<sup>3</sup>

It is because humans today are most susceptible to outside influence that they can be influenced consciously as never before. Their attitudes and beliefs can be shaped without their being aware of it. They are willing and waiting to be motivated because they want to know what is expected of them.

## Security Safeguards Relating to the Individual Decision-Making Process

### *Conditions of Employment*

In many organizations an applicant must sign a form entitled, "Security Conditions of Employment." These conditions are generally aspects of security policy that are highlighted to establish an understanding between the applicant and the organization. Examples of these conditions include the organization's policies on employee identification badges, parking, locker inspections, package inspections, the use of personnel entrances, and others.

In the same programs these security rules and regulations are included in the employee handbook with other general personnel policies. Regardless of the method used to inform employees of organization policy, all employees should be required to complete a form that states that they have read and understood what is expected of them during their employment. This form becomes a permanent part of the employee's personnel record.

### *New Employee Orientation*

The security portion of orientation for new employees serves several purposes, one of which is to psychologically create an image of protection. New employees who begin their jobs with the understanding that the organization takes its protection responsibility seriously will be less inclined to become involved in undesirable activity.

The security orientation should be presented in a positive fashion, stressing that the security system is provided for the welfare of the organization and the employees. It is also recommended that the presentation indicate the organization's strong position when people become involved in security situations. This position should include the organization's policy on criminal prosecution and strict enforcement of the disciplinary system. The new employee orientation sets the stage for further security education, which must be carried out on a continuing basis.

## Security Patrols

One of the primary purposes of security officer patrol is to prevent security incidents both by physically preventing the act and by creating the image that the organization is properly protected. No part of a complex is too remote or too unimportant to receive unannounced inspection patrols by security. Employers who are performing their assigned job and legitimate visitors view the patrolling officers as a support service and derive a feeling of added safety. Dishonest employees and illegitimate visitors will view the officer as

an important reason to refrain from negative behavior. It is well recognized that as visible security patrols increase, the number of adverse incidents decreases.

Signs and notices have significant value as psychological deterrents. Almost everyone has seen and reacted to such community signs as “Beware of Dog” and “Radar Patrolled.” Many security companies use a sign or decal to advertise their presence with the intent of deterring criminal activity. “Premises Under Closed Circuit Television Monitoring and Firearms Prohibited” are examples of signage utilized to deter wrongdoing.

Employee lockers are sometimes receptacles for such items as stolen property, gambling equipment and data, drug abuse paraphernalia, and contraband such as liquor or weapons. A conspicuous sign that indicates locker inspections or one that offers a reward for information leading to the arrest and conviction of people responsible for theft or malicious destruction of property is good advertising. This type of sign reinforces the protection image and can result in receiving good information from concerned staff.

Another method of reinforcing the protection image through signs is the telephone sticker used in many security programs. The sticker generally gives the security telephone number and sometimes numbers for fire or other emergencies. The main purpose of the sticker is to provide personnel with easy access to the correct numbers. People consciously read these emergency numbers while using the telephone for normal calling, at least the first couple of times. After a few times the caller no longer consciously reads the sticker but subconsciously makes note of the numbers, thus reinforcing the protection image. [Figure 2-2](#) illustrates an actual security telephone sticker. One method of attracting conscious attention to the emergency numbers is to change the color of the telephone stickers periodically.

## False Security Expectations

In applying psychological security deterrents there is a difference between inhibiting negative behavior and creating a false sense of security. In the former, the target is the potential perpetrator, and in the latter the focus is on the victims. Creating a false sense of security has legal ramifications. A false sense of security can be created in several different ways but generally involves physical security, signage, or written material that either is false or exaggerates the level of protection provided. Examples of false security are dummy CCTV cameras and signs that claim there is a security patrol or electronic surveillance, when there is not. A false sense of security can occur when security safeguards are compromised or not implemented during a malfunction or temporary absence of a normal safeguard. An example of the latter is a parking lot that is normally protected by a chain link fence. If a section has been removed for construction, an additional safeguard must be implemented to equate the protection normally in place.

**Security Call**  
**(213) 413-3000 Ext. 6767**

**FIGURE 2-2** Sample security telephone sticker.

### *Investigations*

Incident investigation is a very real, tangible security activity that also has certain psychological deterrent ramifications. In some programs the investigation responsibility is taken lightly, with little or no follow-up, especially in the area of property losses. In some facilities a nurse or department supervisor prepares the loss report, which is forwarded to the administration with no further action. If the loss is due to an employee, the perpetrator sees no activity resulting from the crime. The organization conveys the message that it does not care, which makes it easier for the criminal to repeat the crime without inhibition and with little fear of the consequences. Also, in this ineffective system the nurse or supervisor may find it relatively easy to neglect to file a report of the incident because of the perception that nothing will be done.

All protection programs must provide an immediate field response to security incidents. In larger programs a security officer responds to the incident location; in smaller programs an administrative aide, maintenance worker, or nursing supervisor may respond. That someone in authority is concerned and asking questions about the problem is important. A follow-up inquiry is also important in many cases to bring the incident to a successful conclusion.

The objective of any incident investigation is to record the facts properly and to resolve the problem. One should not infer that making a show or going through the motions is the objective. Rather, the demonstration of security is a by-product of proper investigation, and it has positive effects on preventing incidents.

### *Each Malefactor Is Different*

There is no question that each malefactor or wrongdoer is different. The system of physical security and psychological deterrence in the healthcare setting is intended to prevent as many negative acts as possible. The security fence cannot be built high enough to exclude or deter all those who wish to prey on healthcare organizations. How high to build the fence in a particular organization is a management decision based largely on the value or importance that the organization places on security and its risk tolerance.

## Basic Security Program Objectives

Basic objectives of the healthcare security program can be viewed as:

- Contributing to the overall mission of the healthcare organization in the provision of excellent medical care services.
- Preventing security-related incidents through a proactive system of security safeguards.
- Responding to security incidents in such a manner that property damage or injury to persons is prevented or at least mitigated through competent timely actions.
- Creating a sense of confidence in the minds of staff, visitors, and persons being served that they are interacting in a reasonably safe and secure environment.
- Providing services and activities in a positive and effective manner that supports the goals and culture of the organization being served.

The planning and implementation of program elements to achieve these basic objectives are influenced by both internal and external forces.

## Internal Forces

The internal forces of the healthcare organization will be the primary elements of the type, style, and ultimate effectiveness of the operating security system. The four major internal forces are the organization philosophy/culture, leadership, funding, and corporate policy each interacting with each other to shape the program.

### *Organization Philosophy/Culture*

The philosophy and culture of the healthcare organization greatly influence the development and functioning of the security programs. Tradition, cultural factors of the population being served, types of treatment programs, and open versus closed facilities are linked to produce a somewhat unique environment for each individual healthcare organization. While virtually all healthcare treatment facilities strive for achieving market share through an open, welcoming, and patient-centered environment, there is a trade-off in also providing a reasonable level of security and safety. An extremely open environment, which allows the public free and uncontrolled access to the facility, unduly endangers patients, staff, and visitors.

Planetree, Inc. is a nonprofit membership organization founded in 1978 that facilitates the creation of patient-centered care in healing environments. In the Planetree model there is a patient-centered focus as opposed to a provider focus. This model recognizes, in part, facility architecture and design factors which are barrier-free and encourage family participation in patient care and treatment. In principal, most would agree that the model makes good sense until the aspects of barrier-free and inadequate control of public access becomes a significant danger. This danger can create an environment that falls below the standard of care in providing a reasonable and prudent level of safety and security for the healthcare environment stakeholders.

### *Leadership Responsibility*

The leadership of the healthcare organization from the organization's Board of Directors downward through the chain of command ultimately determines the level and type of security program protecting the organization. The well-versed and professional director or manager of security can, however, greatly influence top leadership's perception and thus commitment for a productive security system. Conversely, the ill-informed, ill-prepared, and unqualified security administrator can greatly reduce top management's support through lack of credibility. In the same line of thought, the security administrator who may have sound and progressive ideas/plans must be able to effectively communicate with top management regarding the need and appropriateness of their recommendation in order to move forward. Sound rationale and a plan of implementation generally precede acceptance and program funding. The professional healthcare administrator will

constantly strive to improve business management skills as well as keep abreast of challenges and industry best practices in the field of healthcare security.

In a recent national survey relative to hospital security, less than 20% of the respondents indicated that security was a top priority of upper management.<sup>4</sup> In many respects this extremely low percentage rating can be traced back to both insufficient development (education and training) of healthcare administrators in protection and in general, a lack of sufficient exposure of the healthcare administrator of the benefits afforded by a sophisticated security program. Whatever be the reason, this lack of priority by healthcare organizations is not shared by patients, staff, or visitors who are counting on being safe and secure in “the healing environment.”

### *Funding*

There never seem to be sufficient budgeted funds to implement the healthcare security administrator's security plan. Security budgets compete with clinical care budget requests which at the onset places security budget requests behind the curve. In most cases the budgeting process involves various elements of the Return on Investment (ROI). The term ROI is quite often viewed in dollars and cents. Dollars often predominate over the less tangible ROI aspects of preventing incidents, mitigating damages when incidents occur, the quality and scope of services rendered, and the enhancement of good community/staff reputation and goodwill. Security budgets should always be based on a valid justification of need. Unfortunately, the security budget is often under-resourced until a major incident occurs and suddenly new security funding becomes available—it is reactionary and somewhat akin to rewarding the security budget when bad things happen. Measuring the ROI of deterrence is often the “Achilles heel” for obtaining needed resources.

### *Corporate Policy*

A vast majority of hospital organizations have shifted from being a single, stand-alone type of organization to being an entity of a larger healthcare system. This change has been brought on by mergers, partnerships, or sale of healthcare organizations. As a result of the changing governance of the individual healthcare organization, the direction and philosophy of the security program are subject to a degree of change from minor changes to complete reorganization. While these changes are intended to have a positive effect on the security program of each single entity, that is not always the case. Too often a corporate policy or practice is formulated which works well for a member facility with certain characteristics but is ineffective, inefficient, and possibly a burden on a facility with different characteristics. Included in these different characteristics would be primary types of patient care being provided, population being served, size and location of the facility, the crime environment, and the level of public safety agency support.

Corporate directions and involvement with the individual facility security program will vary according to the management model put into place. These variations can range from minimal impact to a strong central control of policies, procedures, and philosophical

approaches. There are numerous corporate healthcare security system models which are more fully discussed in *Chapter 6, Security Department Organization and Staffing*. [Table 2-4](#) outlines many of the external entities that influence the healthcare security program.

## External Forces

The internal forces influencing healthcare security programs previously discussed must be integrated into a host of external forces or entities such as those shown in [Table 2-4](#). These entities are a mix of trade associations, regulatory agencies, accreditation, and allied healthcare organizations often with conflicting and inconsistent approaches and regulations relative to the security of healthcare organizations.

### The Joint Commission (TJC)

TJC primary security standards are contained within the functional chapter entitled “Management of the Environment of Care” in the Security/Safety Management section.

As part of its Emergency Operations Plan requirements for hospitals, internal safety and security standards during an emergency are also found in the Emergency Management (EM) section. These include making advanced preparations, identifying the role of community security agencies (police, sheriff, national guard), and coordinating their security activities during an emergency. The controlled entrance into and out of the facility, the movements of individuals within the facility, and the control of vehicles that access the facility during an emergency are also addressed.

In addition, there are other standards that have a direct bearing on security in terms of action and compliance requirements. These standards are considered “whole house,”

**Table 2-4** Organizations Influencing Healthcare Security

#### External Entities That Influence the Security Program

- The Joint Commission (TJC)
- National Center for Missing and Exploited Children (NCMEC)
- Occupational Safety and Health Administration (OSHA)
- Center for Medicaid and Medicare Services (CMS)
- International Association for Healthcare Security and Safety (IAHSS)
- ASIS International
- Emergency Nurses Association (ENA)
- National Fire Protection Association (NFPA)
- State Health Departments
- Federal, State, and Local Legislation/Ordinances
- National Health Service (United Kingdom)
- Accreditation Canada
- Australian Commission on Safety and Quality in Healthcare Care

applicable to all hospital staff, and are principally found in the chapters on Human Resources (HR), Leadership (LD), Improving Organization Performance Standards (PI), and Management of Information (IM). The healthcare security administrator must coordinate with other departments and functions to determine specific action items and compliance oversight regarding security standards.

In the area of security, this impact is, however, beginning to erode as TJC in 2009 combined the safety and security standards within the Management of the Environment of Care. This will not improve safety and security but serve only to dilute the protection measures used to make our healing environments safe. The disciplines of safety and security should be separate to promote a safer and more secure environment. As the body of knowledge continues to evolve for each of these disciplines, the educational offerings available will remain separate. There are very few higher education institutions that combine these two disciplines in the same degree program.

TJC surveyors tend to “broad brush” security or to ignore it altogether. It appears that most “surveyors” do not have their arms entirely around security, preferring to address the more defined area of Life Safety.

References to the various TJC security standards will be made in the subsequent discussion on specific elements of the healthcare security program. [Figure 2-3](#) provides an overview of how TJC Environment of Care standards have evolved since 1990.

## National Center for Missing and Exploited Children (NCMEC)

The NCMEC is a private, nonprofit 501(c)(3) organization, established in 1984, to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children.

The number of nonfamily infant (birth to 6 months) abductions from hospitals and birthing centers continues a downward trend. This reduction is due, in large part, to the efforts of the NCMEC. The work of John Rabun (Vice President and Chief Operating Officer) and Cathy Nahirny (Administrative Manager of the Jimmy Rice Law Enforcement Training Center and staff of the NCMEC) has provided the tools and support to prevent infant abductions. It was not until 1987, when the NCMEC studied the problem of infant abductions, specifically from hospitals, that the extent of these incidents was known. Their study data began in 1983 and their research and tracking continue as an ongoing NCMEC program.

The NCMEC does not just study the problem but provides ongoing training and education and is an instant resource to facilities and law enforcement agencies when an abduction occurs. The work of the NCMEC goes far beyond hospital abductions; however, for the purposes of this text, the focus is on nonfamily abductions within the healthcare delivery system. The delivery system involves some four million plus births each year in approximately 3,500 US birthing facilities with care continuing to a limited degree after discharge in the home environment. Hospital-operated, or independent, home healthcare agencies frequently provide aftercare to mother and baby in the home. The healthcare security administrator must also be aware that there can be a certain degree of organizational



**The Joint Commission Environment of Care Time Line**

<p><b>1990–1992</b> Plant Technology and Safety Management, and Statement of Construction in existence</p>	<p><b>2004</b> Complete revision and reorganization of standards, organized as:</p> <ul style="list-style-type: none"> <li>• Planning and implementation</li> <li>• Measuring and improving</li> </ul> <p>New scoring system issued Measures of success added “Shared Visions-New Pathways” survey process introduced, including:</p> <ul style="list-style-type: none"> <li>• Triennial survey and periodic performance review</li> <li>• Tracer methodology</li> <li>• Environment of Care Interview replaces Environment of Care Document Review</li> <li>• Construction issued added to EC Interview</li> <li>• Corrective action plan required in 90 days</li> <li>• Requirements for improvement cutoffs added for accreditation decisions</li> </ul>
<p><b>1993</b> Standards revised and reformatted Plant Technology and Safety Management retitled as “Management of the Environment of Care,” which includes:</p> <ul style="list-style-type: none"> <li>• EC.1: Design</li> <li>• EC.2: Teach/implement</li> <li>• EC.3: Measure/assess</li> <li>• EC.4: Other environmental considerations</li> <li>• EC.5: Smoking</li> </ul> <p>Statement of Construction retitled “Statement of Conditions” Random unannounced surveys initiated</p>	
<p><b>1996</b> Sentinel Event policy released</p>	<p>Risk assessment emphasized Workplace violence and infant abduction requirements added</p>
<p><b>1999</b> Building Maintenance Program becomes available</p> <p>Performance Standards become “Performance Monitoring” Expanded testing of features of fire protection with National Fire Protection Association references</p>	<p>Department of Transportation requirements added as applicable law and regulation footnote Involvement of leadership and medical staff required in emergency management 2000 Life Safety Code adopted</p>
<p><b>2001</b> Standards reformatted to include:</p> <ul style="list-style-type: none"> <li>• EC.1: Planning</li> <li>• EC.2: Implement/teach</li> <li>• EC.3: Other environmental considerations</li> <li>• EC.4: Monitor/improve</li> </ul> <p>Worker safety reconfigured as separate standard Smoking moved under safety standard Environmental Protection Agency and Occupational Safety and Health Administration cited as examples of applicable law and regulation</p> <p>Emergency Preparedness becomes “Emergency Management” and includes:</p> <ul style="list-style-type: none"> <li>• Incident command</li> <li>• Hazard vulnerability analysis</li> <li>• Community integration</li> </ul> <p>Airborne contaminants and waterborne pathogens added to utilities standard</p> <p>Training issues consolidated to one standard</p> <p>“Accreditation with Commendation” eliminated Patient safety standards announced</p>	<p><b>2005</b> 45 days for corrective action plan initiated Scoring modifications issued Addition of Life Safety Code Specialists to survey Addition of competency requirements for person completing Statement of Conditions Medical equipment maintenance based on life support and non-life support Utilities maintenance based on life support, infection control support and non-life support</p>
<p><b>2002</b> Emergency Management “clarifications” issued in response to 9/11</p>	<p><b>2006</b> All surveys unannounced Emergency Management Observation added to survey Identified observer added for emergency exercises Changes to emergency exercise critique requirements</p>
<p><b>2003</b> Communitywide emergency drill added Preconstruction Infection Control Risk Assessment added First National Patient Safety Goals issued</p>	<p><b>2007</b> Addition of validation surveys</p> <p><b>2008</b> All hospitals surveyed by Life Safety Code Specialist</p> <p>Hospitals over 750,000 square feet surveyed by Life Safety Code Specialist for two days</p> <p>Total rewrite of emergency management requirements, including:</p> <ul style="list-style-type: none"> <li>• Inventory issues</li> <li>• Stand-alone capability</li> <li>• Security issues</li> <li>• Communications</li> </ul> <p><b>2009</b> Total rewrite of all standards with emergency management and Life Safety Code compliance as separate chapters in accreditation manual Combination of Safety and Security into one standard</p>

**FIGURE 2-3** TJC Environment of Care standards time line (reprinted with permission from *Health Facilities Management Magazine*).

responsibility for infant safety in the home after discharge from the hospital. In the event information, actions, or inactions on the part of the healthcare organization caused or contributed to a criminal act in the home, there could be certain legal ramifications.

## Occupational Safety and Health Administration (OSHA)

Worker safety is the primary focus of OSHA in contrast to patient safety which is the focus of TJC. Under the Occupational Safety and Health Act of 1970, employers are responsible for providing a safe and healthy workplace for their employees. Although OSHA is a federal regulatory agency, individual states may create a state OSHA agency which, in general, must equal or exceed federal requirements. OSHA's stated role is to promote the safety and health of America's work force by setting and enforcing standards; providing training, outreach, and education; establishing partnerships; and encouraging continued process improvement in workplace safety and health. The vast resources of OSHA and its state partners include approximately 2,100 inspectors, plus complaint discrimination investigators, engineers, physicians, educators, standards writers, and other technical and support personnel in over 200 offices.

The major impact of OSHA relative to security relates to workplace violence as it affects staff. An initial and primary document produced by OSHA is "Guidelines for Preventing Work Place Violence for Health Care and Social Service Worker" (OSHA 3148, 1996). The National Institute for Occupational Safety and Health (NIOSH) has published "Violence: Occupational Hazards in Hospitals," April 2002, which is also a significant reference for the security practitioner.

There is a formal joint working relationship between OSHA and TJC. This relationship is defined in the OSHA and TJC/Joint Commission Resources Alliance. The Joint Commission Resources (JCR) is the official publisher and educator of TJC.

## Centers for Medicare and Medicaid Services (CMS)

The CMS impact on healthcare security more often than not is in relation to a major security incident occurring in an approved provider facility. The ensuing investigation by CMS contracted staff (i.e., State Health Departments) in many cases results in ill-informed and ill-conceived changes in the CMS standards/rules which can have the effect of actually decreasing the overall protection level being provided for patient, visitor, and staff by the provider organization. An example is the "attempt" by CMS to define the difference between law enforcement restraint devices and patient care restraint devices and their "appropriate" use.

## International Association for Healthcare Security and Safety (IAHSS)

This Association is the primary resource that shapes, designs, and affects the scope of practice in healthcare security. It was formed in 1968 as the International Association for Hospital Security and in 1990 changed to the IAHSS. It was incorporated in the State of Illinois in 1968 as a private, not-for-profit organization.

The first annual meeting of the Association was held in June 1968 at the New York Hilton. In addition to the business meeting there was a panel/attendee discussion on what security functions and responsibilities were appropriate to a hospital security department. There was a consensus of those present that these responsibilities included those shown in [Table 2-5](#), Hospital Security Functions and Responsibilities in 1968.<sup>5</sup>

This bit of history indicates how the field of healthcare security has changed over time eliminating certain functions, maintaining certain functions, while adding new areas of responsibility.

The IAHS has evolved into a major association with a sharply defined focus recognizing that the healthcare environment has unique security risks and vulnerabilities. There are currently over 1,800 members of the association working together to improve the management of healthcare security programs. While the accomplishments of IAHS are many, the association is especially strong in its security officer training programs, the credentialing of management-level personnel, and the development of Healthcare Security: Basic Industry Guidelines.

In 2007, the Association introduced a new organizational structure to better align resources including their strong voluntary leadership. The new structure created a Commission on Certification, a Council on Education, a Council on External Affairs, and a Council on Membership.

**Table 2-5** Hospital Security Functions As Identified by IAHS in 1968

**Hospital Security Functions and Responsibilities in 1968**

- (1) Uniformed patrols
- (2) Elevator operators
- (3) Information desk
- (4) Lost and found
- (5) Key control
- (6) Identification
- (7) Fingerprinting
- (8) Education of employees in safety and fire protection
- (9) Accident reports on hospital grounds
- (10) Manual of procedures
- (11) Disaster procedures
- (12) Training security officers
- (13) Alarm systems
- (14) Maintaining good relations with official police
- (15) Transportation
- (16) Decreased patient property

**PREAMBLE****HEALTHCARE SECURITY: BASIC INDUSTRY GUIDELINES**

Healthcare facilities (HCFs) and healthcare organizations (HCOs) are responsible for providing a safe and therapeutic environment while respecting the rights and privacy of those entrusted to their care. These guidelines are intended to assist healthcare administrators in fulfilling their obligation to provide a safe, secure, and welcoming environment, while carrying out the mission of their healthcare organization.

HCF, for purposes of these guidelines, shall mean any facility used in providing healthcare service or treatment simultaneously to four or more patients

- who may be primarily incapable of self-preservation due to physical or mental limitation;
- who are undergoing treatment or testing which may temporarily render a patient incapable of taking effective action under emergency conditions without assistance from others.\*

These guidelines support the need to comply with all national, state/provincial, county, and local requirements and are intended to be in harmony with all regulatory, accreditation, and other healthcare professional association requirements and guidelines.

These guidelines are periodically reviewed by the IAHSST Guidelines Task Force. Changes, modifications, and new guidelines are posted on the IAHSST website, upon being approved by the IAHSST Board of Directors.

Comments and suggestions are encouraged and may be directed to the IAHSST Guidelines Task Force, P.O. Box 5038, Glendale Heights, IL 60139.

---

\*National Fire Protection Association [NFPA] #730—guide to Premises Security.  
Copyright 2009 by IAHSST, P.O. Box 5038, Glendale Heights, IL 60139.

The development of basic guidelines is the responsibility of an established Association Guidelines Committee. This Committee is comprised of members from various settings of the healthcare environment to include representation of large, small, and university-affiliated facilities, contract providers, and consultants.

The IAHSST basic security guidelines are especially important to the forward movement of healthcare security. They provide a consensus approach to the basic fabric and direction of the structure of this emerging discipline: a discipline that is an essential element in the provision of excellence in patient care.

The Preamble to the security guidelines provides an explanation of the purpose and detail regarding the application of the guidelines. The Association publishes an annual booklet containing the guidelines; however, as these guidelines are subject to continuous review and changes, the Association website ([www.IAHSST.org](http://www.IAHSST.org)) contains the most current and up-to-date information.

The statements and intents of these guidelines are designed to be applicable to all HCFs. It is recognized, however, that the actual implementation of these guidelines will vary from facility to facility—dependent upon, among other considerations, the nature, size, and location of the facility and the reasonably foreseeable risks to be protected against.

#### *ASIS International*

ASIS International (formerly the American Society for Industrial Security), founded in 1955, is the world's largest organization for security professionals, with more than 36,000 members worldwide. This organization embraces virtually all aspects and environments of security through 31 volunteer councils. One of these councils is the Healthcare Security Council. The stated purpose of this Council is to provide credible resources and information on healthcare best practices, including physical security, staffing, and sample policies and procedures. Although not specific to healthcare security, ASIS International has developed a number of guidelines and standards that serve as a resource for the healthcare security practitioner. ASIS International is an accredited Standards Developing Organization conferred by the American National Standards Institute (ANSI). As such, ASIS International actively participates in international standard initiatives as a member of the International Organization for Standardization (ISO).

Security standards and guidelines that are currently available or pending committee action are:<sup>6</sup>

- Business Continuity
- Business Continuity Management
- Chief Security Officer
- Facilities Physical Security Measures
- Facilities Physical Security Management
- General Security Risk Assessment
- Information Asset Protection
- Pre-employment Background Screening
- Private Security Officer Selection and Training
- Risk Assessment
- Security, Preparedness, and Continuity
- Threat Advisory System Response
- Workplace Violence Prevention and Response

Although the standards and guidelines are not specific to healthcare security, they serve as a valuable information resource, at least in part, for adaptation to the healthcare sector.

#### *National Fire Protection Association (NFPA)*

The NFPA is an international, not-for-profit organization established in 1896 for the purpose of reducing the burden of fire and other hazards on the quality of life by providing and advocating consensus codes, standards, research, training, and education

as a trade association. Organizational membership totals more than 81,000 individuals around the world and more than 80 national trade and professional organizations. It is the world's leading advocate of fire prevention and an authoritative source on public safety. Their codes and standards are regularly adopted by licensing/regulatory/accreditation and public safety agencies who become the legal enforcement entity for such standards.

In terms of the healthcare security, one of the most utilized NFPA codes is the Life Safety Code 101. It is this code adopted by most fire Authorities Having Jurisdiction (AHJ), TJC, CMS, and licensing authorities that significantly impact security systems, design, and operations.

In a relatively recent endeavor the NFPA has published NFPA 730, Guide for Premises Security, 2008 edition. In this document Chapter 12 is entitled "Health Care Facilities." The information contained in the two pages devoted to healthcare in this 82-page document is very general and in some cases not always practical. As an example, Section 12.4.4.5(E) states, "burglar alarms, fire alarms, and video surveillance systems should be monitored at a central station console that is constantly manned." This standard would not only be impractical but cost prohibitive and virtually impossible for the small healthcare facility that does not even maintain a security force.

## State Health Departments/Legislation/Ordinances

Virtually all states in the United States and most other countries' political/government subdivisions have entities that license or oversee healthcare services. A role of the State Health Department that bears directly on healthcare security is that of licensing and a contract with CMS for certain services. These services include follow-up inspections and investigatory activity. As with any regulatory or quasi-regulatory authority, new and changing license requirements can emanate from crisis situations or incidents. Directed changes in license requirements, often with short turnaround times, are a result of this reactionary investigative activity.

The passage of the federal law, Patient Safety and Quality Improvement Act of 2005, has resulted in numerous healthcare reporting systems in both state and federal mandated reporting healthcare errors relating to patient safety.

The National Quality Forum (NQF) has been a leader in establishing a list of the types of healthcare errors that need to be reported and evaluated. The NQF publication "Serious Reportable Events in Healthcare—2006 Update: A Consensus Report,"<sup>7</sup> identifies 28 adverse events that are serious, largely preventable, and of concern to healthcare providers, consumers, and all stakeholders. Events are grouped in six categories. The two categories of direct interest and general involvement of security are:

### Patient Protection Events

- Infant discharged to wrong person
- Patient death or serious disability associated with patient elopement (disappearance)

- Patient suicide, or attempted suicide, resulting in serious disability while being cared for in a healthcare facility

#### Criminal Events

- Any instance of care ordered, or ordered by, someone impersonating a physician, nurse, pharmacist, or other licensed healthcare provider
- Abduction of a patient of any age
- Sexual assault of a patient within or on the grounds of a healthcare facility
- Death or significant injury of a patient or staff member resulting from a physical assault (i.e., battery) that occurs within or on the grounds of the healthcare facility.

In addition to being knowledgeable of federal and state legislation affecting health-care security, the security practitioner must consider any local laws or ordinances. As an example, some municipalities have enacted ordinances relative to the provision of security in parking facilities.

In summary, it is the responsibility of the healthcare security administrator/practitioner to diligently research such laws and ordinances that may affect the provision of security services for the healthcare organization.

## External Influencing Agencies (Non–United States)

Outside of the United States, there are legislative provisions, accrediting organizations, and licensing entities that influence healthcare security in their respective countries, such as in the United Kingdom, Canada, and Australia.

### *United Kingdom*

In 2003, the National Health Service (NHS) in the United Kingdom created the Security Management Service and provided them with legislated authority over all healthcare security issues across the NHS in England—the first time a dedicated organization has had such a charge. This includes:

- Protecting NHS staff from violence and abuse;
- Taking appropriate action against those who abuse, or attempt to abuse, NHS staff;
- Helping to ensure the security of property, facilities, equipment, and other resources such as drugs;
- A defined operational structure for security management.

The remit of the NHS Security Management Service extends to the protection of all NHS resources—which include staff, facilities, equipment, drugs, and even items such as the radioactive materials used in some operations.

The Care Quality Commission was established by the Department of Health of the United Kingdom to promote and drive improvement in the quality of healthcare and public health in England and Wales. Independent of the NHS, the Care Quality Commission is an independent regulator of health and social care in England.

*Canada*

If TJC is viewed as perhaps the key external influence on healthcare security in the United States and the Security Management Service conceded as the centralized national authority in this area in the United Kingdom, it is important to view Canadian healthcare security through a different lens, one where there are a number of local, provincial, and federal bodies influencing policy and practice.

Like most countries Canada has regulatory requirements around many professional and specialized fields in healthcare that can impact on the healthcare security profession—narcotic control measures and protection of radioactive materials are relevant examples. Canada is not unique in that building and fire codes exert significant regulatory influence over designing healthcare facilities for security and in healthcare staff training in preventing and responding to emergency events such as fire alarms.

However, if we look for standards and regulation around healthcare security in the Canadian milieu, we discover a patchwork of provincial and local health jurisdiction initiatives, both formal and informal, that serve to loosely govern and influence the healing environment. With respect to established standards for training security personnel in Canada, including healthcare security personnel, a growing trend is found, from province to province, toward training and licensing requirements that can be viewed as an inexorable march toward professionalizing the industry. However, these standards differ from province to province and are managed and monitored by provincial bodies in each jurisdiction. It is often left to healthcare organizations and/or private security companies to build on these baseline standards to manage the complexities that confront security personnel in healthcare.

Accreditation Canada, the healthcare accreditation body for the Canadian healthcare industry, is relatively silent in the application of standards for healthcare security. Unlike TJC, which applies rigorous standards in a defined review process, there are no Canadian requirements for Security Management Plans, as an example, and security programs are not evaluated on their own but rather as a component of a broader review such as patient/client safety or emergency response capacity. While the fire safety and emergency management disciplines have well-defined standards to address through the Accreditation Canada process, the security function does not. However, just as there is a clear Canadian trend toward mandatory training and licensing requirements for security personnel, there is also a movement within some Canadian healthcare entities to ensure the development of a professional program that would meet Joint Commission-like standards should the Canadian process evolve in that direction. The IAHS HealthCare Security: Basic Industry Guidelines are a good example of a tool available to Canadian healthcare security program leaders to support a move in this direction.

According to Don MacAlister, Executive Director of Protection Services and Emergency Management for Fraser Health and Vancouver Health in British Columbia, there are other regulatory and nonregulatory bodies that yield significant influence on the Canadian healthcare security industry. The Worker's Compensation Boards of Canada influence the risk assessment processes and the ability of an organization to respond to aggression in healthcare, as an example. This, in turn, will impact areas such as security



design, training, and even security staffing levels in some cases. It can be argued that healthcare unions—and in particular nurses unions in Canada—play a significant role in shaping security measures and, by extension, the healthcare security programs in many jurisdictions. The unions have been successful, in some provinces, in negotiating provisions in their collective agreements that influence healthcare security policy and practice. This involvement can include the development of policy and protocol around “flagging” potentially violent persons, on the practice of police laying charges against those who assault staff, and even exerting influence on the design of secure environments in Canadian hospitals.

So, while there is no single influencing body in Canada as there are in the United States and the United Kingdom, it should be clear there are a number of governmental and nongovernmental agencies that yield considerable influence over the healthcare security industry in Canada.

### *Australia*

The Australian Commission on Safety and Quality in Healthcare Care was established on January 1, 2006, by Australian Health Ministers to develop a national strategic framework to improve safety and quality across the healthcare system in Australia. The Commission’s role is to lead, coordinate, and monitor improvements in the safety and quality of patient care. The Commission takes on educational and standards-setting role as it disseminates knowledge and advocates for safety and quality. Like TJC, the Commission has specific standards and reports on sentinel events occurring in Australian hospitals.

## Body of Knowledge

All disciplines, including healthcare security, develop a “body of knowledge” over time. One of the basic criteria for a defined profession is a “body of knowledge” that is generally accepted by the majority of persons operating within a specific discipline. There is a difference between the term *profession* and the term *professional*. While the healthcare security discipline may not yet have all the ingredients of a true profession, it should be the practitioner’s goal to act in a professional manner. In this respect, the healthcare security practitioner must maintain a current “working knowledge” of the general principles of healthcare security. A display of professional conduct by practitioners is a precursor to achieving a professional discipline that is accepted as such by the general population.

### Developing “the Knowledge”

The development of the vast body of knowledge in healthcare security has gradually taken place on a formal and informal basis. This development of information defines and shapes the accepted concepts of today’s successful security program. Commonly accepted principles evolve which become generally accepted both by persons within and outside the discipline. The healthcare security discipline has been building a body of knowledge for several

centuries with its roots well established in England. This healthcare body of knowledge has changed dramatically during its life and occasionally makes strange twists and turns.

An example of a dramatic change for healthcare security occurred in about the middle of the twentieth century. At that point in time healthcare security was primarily viewed as a law enforcement function operating somewhat outside the sphere of the healthcare delivery system. Over a short period of time, in the mid- to late 1960s, healthcare security became integrated into the healthcare delivery system, becoming an important stakeholder within the “healthcare team.” Today security, in virtually all disciplines, is viewed as an important function and is only generally associated with the criminal justice aspects of years gone by.<sup>8</sup>

### Accessing “the Knowledge”

Where does one find this body of knowledge? It is found in the literature, in the classroom, at seminars and workshops, in litigation proceedings, in accreditation/regulatory requirements, in healthcare security departments, and in the minds of healthcare security practitioners. All this accumulated knowledge is subjected to interpretation and evaluation leading to a general consensus within the discipline. This knowledge is then loosely translated into basic elements. These elements are then transformed, and more precisely viewed, as *industry standard practices*, *best practices*, and a *standard of care*. These three terms are distinct, and different, yet have a linkage or relationship to each other. Their definitions and meanings help us in “organizing” our healthcare security body of knowledge.

#### *Industry Standard Practice (ISP)*

An ISP is an operational plan or activity that is common to healthcare security operations as a basic concept or premise. As such the implementation of the ISP may vary in detail unique to an individual facility or organization but will generally produce, or is intended to yield, a common outcome. An example of a healthcare ISP is to provide designated security officer coverage in the hospital setting. This practice is applicable to most hospitals; however, it should be noted that some very small facilities located in rural areas, or in very low crime areas, may not need the services of designated security officer coverage. They do, however, need to have a plan for security and especially a plan for response to security-critical incidents. Another ISP is the training and education of all facility staff. Staff must be trained in the basics of organizational security and their individual responsibility in support of the overall security program.

Industry security practices may emanate from outside sources such as accreditation/regulatory organization (i.e., CMS, OSHA, TJC, State Health Departments) and resource organizations that have developed information with relevancy to healthcare security (i.e., NCMEC, NFPA, ASIS, IAHS). The NCMEC efforts in regard to infant abductions is a good example of how an outside resource can shape an ISP and even relate directly to a standard of care. Their publication, “For Healthcare Professionals: Guidelines on Prevention of and Response to Infant Abduction,” 9th Edition, 2009, in effect sets a

nationally recognized healthcare security standard.<sup>9</sup> The support of the “guidelines” by various organizations, as shown on the cover of this document, provides a strong consensus of agreement in this very important area of healthcare security. It is perhaps one of the most “prescriptive” of our ISPs which has *de facto* transitioned into a basic standard of care involving hospital infant security.

### *Best Practice*

A *security best practice* is an act, procedure, or operational activity that tends to validate its worth (merit, value, useful) with demonstrated repetition. A best practice is often associated with a practice that is utilized in the majority of protection programs; however, in fact, in itself, it should not be the sole evaluative criterion. The term *benchmarking* should not be viewed as having the same meaning as “best practice.” In many instances benchmarking merely means a comparison of statistics which produce interesting data but does not correlate to a best practice. On the other hand, an example of a healthcare security best practice is the manner in which security officers are attired. It is generally accepted that a standard security/police uniform (uniform versus soft clothes) is an industry best practice. In this case the majority of healthcare security officers are uniformed in traditional military-style attire in over 90% of our nation’s healthcare security programs. This practice has met the test of value and usefulness over time.

Another example of a security best practice is the picture identification type of badge to be worn by healthcare staff. It is a healthcare standard (both security and clinical care provider requirement) that staff be properly identified. In complying with this standard a color photograph of the person, position, and proper display of an identification badge have become security and business best practices.

There is a direct linkage between the security ISP and organizational best practice. Not all best security industry practices involve just security personnel alone. They can, and will, often involve other organizational staff. The elopement (missing) patient provides a clear illustration of this point. One of the standards of care in terms of a missing patient is to conduct a timely and thorough search. An ISP is to involve general staff as well as security personnel. The best practice is to have assigned areas of search. A basic practice is to have security and/or maintenance personnel begin their search of the perimeter of the facility and work inward while clinical and other staff conduct the internal search moving outward.

### *What Are Standards?*

Standards are voluntary, or legally mandated, guidelines and best practices that improve the quality and consistency of goods and services. They provide predictable action and reactions as well as direction and control of security operations in managing manmade and national security risks and vulnerabilities. Standards are essential in advancing the discipline of “healthcare security” toward the goal of stakeholder understanding and participative support in the long road to a professionally established status.

### *National Standard of Care*

The term *standard of care*, in relation to security, refers to the protection level in place under the conditions of the specific security risk at any given point in time. The security standard of care is a level of protection in place in terms of being reasonable and prudent in view of all circumstances. The term *standard of care* is often referred to when an event has taken place; however, its meaning and application are not limited to an event. As we are aware, the level of protection provided by the healthcare organization is dynamic in that it flexes between meeting the standard of care for the referenced risk and falling below the standard of care. There are endless examples that illustrate this flex concept—for example, locking hospital nursery doors at all times and equipping them with self-closing (latching) devices to meet the security standard of care. For sake of discussion let us assume that during one morning it was discovered that the self-closing device was not functioning properly (this is often referred to as an “engineering failure” by some). At this point in time the security standard of care is breached and the level of protection does not meet the acceptable standard of care. Short of immediate repair of the device, the meeting of the standard of care could be restored by implementing a new (generally temporary) security safeguard that provides protection that meets or exceeds that of the failed safeguard. In this illustration a person, unit staff, or security officer could be assigned to monitor door activity until equipment repair is accomplished to maintain an acceptable standard of care.

### *Standard of Care—Organization Specific*

In addition to the national security standard of care, a healthcare facility (or system) will often develop a protection system that, in part, exceeds that of the national standard. This situation develops as we often ascribe to the adage that “more security is better.” In all probability it does, however, raise the bar in terms of the security standard of care for a specific organization.

### *Common Goals*

It is not uncommon that regulatory, legislative, or local fire department edicts conflict with established security standards of care. These situations must be addressed with all parties to find a workable solution to these conflicts of interpretation. An example of such a conflict was experienced by a hospital in a Chicago suburb. The Village Board enacted an ordinance mandating that interior stairwell doors be unlocked in buildings taller than four stories. The hospital (nine stories) could not comply with the ordinance and still meet the security standard of care regarding such areas as labor and delivery, pediatrics, and a closed psychiatric unit. The ordinance was passed as a “knee-jerk” reaction to a fire in another community. Later the Village Board enacted an ordinance that allowed specific stairwell doors of the hospital to be locked but stipulated that in the event of a fire alarm activation, the doors would be electrically unlocked. While these conflicts do occur with a certain frequency, both security and safety entities must have the common goal to prevent property loss, injury, and deaths with good faith problem resolution which can result in meeting the security standard of care.

## References

1. Cohen, D. (2006, May 1). A howling success Security Products. Retrieved June 13, 2009, from <http://secprodonline.com/Articles/2006/05/01/A-Howling-Success.aspx>. (Note: No volume or issue # provided online.)
2. Clark, J. P., & Hollinger, R. C. (1980). Theft by employees. *Security Management* (September).
3. Whyte, W. H. (1956). *The organization man*. New York: Simon and Shuster.
4. Weronik, R. (2008, January 21). Securing our hospitals: GE security and IAHS healthcare benchmarking study. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
5. Annual meeting held in New York. (1968, September). *International Association for Hospital Security Newsletter*, 1(1), 1.
6. ASIS. (2008). Guidelines updated, draft released. *ASIS Dynamics Newsletter* (November/December), 16–17.
7. National Quality Forum. (2007, March). *Serious reportable events in healthcare 2006 update*. Washington, DC.
8. James, R. (2004). Higher education and security management. *Security Products*, 8(January).
9. National Center for Missing and Exploited Children. (2009). *For healthcare professionals: Guidelines on prevention of and response to infant abduction, 9th edition*. Retrieved June 13, 2009, from [http://www.missingkids.com/en\\_US/publications/NC05.pdf](http://www.missingkids.com/en_US/publications/NC05.pdf).

# Security Risks and Vulnerabilities

The foundation of a healthcare organization protection system is the identification and assessment of the types of threats and the degree (impact) of damage if the threat becomes an actual occurrence. Damage includes the impairment of the usefulness of property including destruction, loss, and personal injury including death. Threats may be natural disasters or manmade actions such as accidental incidents or criminal actions. When a threat progresses to an actual event, the organizations viability is diminished in varying degrees depending on the magnitude and seriousness of the resulting damage.

The terms *threat*, *risk*, and *vulnerability*, in the context of security, are often used somewhat interchangeably just as the terms *policy* and *procedure* are more often than not treated as being the same. On close examination, however, each term has a specific and different definition. The important fact is that threats, risks, and vulnerabilities be identified, measured in terms of degree of probability, and the degree of impact on the organization. Appropriate security safeguards must be in place or developed to properly manage (prevent or mitigate) damage to the organization's property and personal safety of the stakeholders.

The term *Hazard Vulnerability Analysis (HVA)* is frequently referred to in the management of healthcare organizations. This term includes security vulnerabilities as a subsection of the broader, more inclusive hazards commonly considered a part of the risk management or emergency management responsibility. The healthcare organization utilizes the HVA as a basis for defining the preparedness and mitigation activities that will mobilize and manage essential resources. For the purposes of this text the term *risk* will be utilized to describe the types of risk, which are basically incident-driven such as theft, assault, abduction, vandalism, fire, flood, and other natural disasters. The latter events are sometimes more appropriately evaluated and managed under the emergency management function while the potential incidents of manmade/criminal acts are more directly the responsibility of the security program. In this chapter the focus will be on the criminal or security type of incident.

Once the security risks (types) are identified they must each be evaluated in terms of probability of occurrence. The probability of occurrence of a specific security risk may vary significantly when viewed in terms of location within the facility. As an example a food service worker in the facility cafeteria, during the noon lunch period, would be less likely to be assaulted than a female staff person working alone at night in a remote location or the staff person going to a vehicle during the night hours. Security risks should

be evaluated not only in terms of probability but also in terms of the consequences or the degree of damage that may result from such an occurrence. A properly conducted security assessment of the organization is essential in identifying security exposures in a methodical manner so that a security system is based on a valid analysis rather than the last security incident. Security incidents do, however, provide important “lessons learned” and are helpful in determining the need for modification of the security system.

## Basic Healthcare Security Risks/Vulnerabilities

All healthcare facilities, regardless of size, are subject to basic security risks. These risks have been grouped into some 21 major categories for the purposes of this text. The magnitude of each risk category, which varies to a considerable degree from facility to facility, determines the threat to the organization. The risks identified in [Figure 3-1](#) must be individually assessed by each facility. These risks can be viewed as being primary security risks while acknowledging that there are also safety security risks involved with the security program.

## Primary Security Risks

Healthcare organizations have their own set of security risks inherent in securing a patient care facility. The following defined risks are found in most healthcare facilities. The risk levels will, however, vary according to the unique operating environment of the organization.

### Assaults

*An assault is the unlawful intentional inflicting, or attempting or threatening to inflict, injury upon another.*

All healthcare facilities face the multifaceted and extremely acute problem of assaults to patients, staff, and visitors. The risk of assault for purposes of this category can be viewed in terms of simple assault or aggravated assault, which includes sexual assaults. The simple assault involves the threatening of injury to another while the term *aggravated assault* refers to the actual striking or touching of another with the intent to inflict serious injury or harm. Assaults can take place inside facilities and on the grounds. Incidents range from simple threats to rape. Serious assaults get immediate attention by administration and account for a large number of lawsuits against healthcare facilities where a security issue is involved.

Patients are particularly at risk to attack due to their physical and mental condition in addition to the fact that they are very accessible. A person would never check into a hotel and go to sleep at night with the corridor door open, yet in a hospital patients do just that, with the added problem that they are sick or injured and thus less able to protect

<b>BASIC HEALTHCARE SECURITY RISKS/VULNERABILITIES</b>	
<b>Assault Grounds*</b> —Internal —External	<b>Kidnapping/Abduction</b> —Stranger —Domestic
<b>Bomb Threat/Bombing</b>	<b>Labor Actions</b> —Slowdowns —Strikes
<b>Burglary</b> —Facilities —Vehicles	<b>Loss of Critical Information</b>
<b>Dissident Group Actions</b> —Demonstrations —Civil Disturbance —Sabotage	<b>Patient Elopement</b>
<b>Disturbances</b> —Internal —External	<b>Robbery</b> —Internal —External
<b>Drug Abuse/Loss</b>	<b>Stalking</b>
<b>Embezzlement</b>	<b>Terrorism</b> —Against Facility —Collateral Damage
<b>Fire/Explosions</b>	<b>Theft (from)</b> —Patient —Staff —Visitor —Facility/Organization
<b>Hostage Taking</b>	<b>Vandalism</b> —Internal —External
<b>Homicide</b>	
<b>Identity Theft</b>	
<b>Imposter</b>	
<b>Kickbacks/Fraud</b>	

\*Includes Sexual Assault

**FIGURE 3-1** Basic healthcare security risks and vulnerabilities.

themselves. The patient is at risk of assault by another patient, a visitor, or even the legitimate caregiver charged with rendering care to the patient. The caregiver is responsible for the majority of assaults against hospital in-patients, particularly in the area of sexual assault. These incidents run the gamut of fondling of a patient in the dentist chair to the reported rapes of patients in a recovery room by a recovery room nurse. Nursing home patients are also at risk relative to rough handling (assaults) and sexual assaults. At a long-term care facility in Pennsylvania, two male patients shared a room when one viciously attacked the other with a wooden chair in hopes to keep the nursing staff from “giving him drugs.”<sup>1</sup> A pediatric nurse at a southern California children’s hospital pled guilty to molesting a 4-year-old comatose patient and trafficking child pornography. A second staff



person, a respiratory therapist, at the same hospital, was charged with posing or modeling children to create child pornography.<sup>2</sup>

A Syracuse, NY, man released from prison was arrested and charged with the rape of a 15-year-old hospital patient. The man entered the hospital during visiting hours with another man to visit the victim's roommate. When the other man and patient left the room the roommate was attacked by the rapist.<sup>3</sup>

It is not always the patient who is the victim of assault. Healthcare staff and visitors are also at risk. Examples include a nurse who was pulled from a stairwell in a construction area and raped, and a visitor was sexually assaulted in a parking structure.

Although sexual assaults command the most attention, other assaults also occur. These include assaults between patients and staff, between staff and visitors, and among family members.

Hospital emergency department and psychiatric treatment areas are frequently the scenes of assaults on staff. Within the hospital, nurses and ancillary staff often work alone at night in remote areas or have a need to travel through these types of areas. Some nursing units may have only two staff members on duty. When one staff member is absent from the unit on an errand or a break, the other may be at risk. In a south Florida hospital a hospice patient appeared at the nursing station and beat the two nurses on duty so severely that both required lengthy in-patient medical treatment.

The assault problem is also evident outside the facility. The facility grounds, parking facilities, and streets surrounding the facility may offer opportunities for assaults to occur. Healthcare organizations can experience difficulty in recruiting staff for the evening and night shifts because of the security risk to staff. It is not uncommon for organizations to provide patrols on nearby streets, and many offer escort services to bus stops and nearby residential areas for employees and visitors. Escorts walk people to their destination or in many programs a vehicle shuttle service is provided.

The home healthcare provider is also at risk of assault. In most cases the home healthcare provider works alone and can find himself/herself in a situation that results in serious injury and even death. Such was the case when Waneta Boatwright, a home healthcare nurse, went to a rural Kansas home to provide care for an elderly woman. What she discovered were two bodies on the floor. She dialed 911 but the call was disconnected. Arriving authorities found the 23-year-old son in the house. The two deceased victims were on the floor and the visiting nurse care provider had also been shot and killed. The son pulled a gun on the officers but was arrested without incident.<sup>4</sup>

## Bomb Threats

*The use of an explosive or incendiary device with willful disregard for the risk to persons or property.*

Bomb threats involving healthcare facilities are not as prevalent today as they were in the late 1960s and 1970s. However, the risk is very real, requiring constant readiness in

dealing with this security problem area. The motives for such threats range from extortion, to revenge, to the excitement of causing trouble, to labor unrest and disgruntled employees, along with the ever-present concerns of the potential for a terrorist attack.

Despite the number of bomb threat calls, seldom are two calls exactly alike. Each call must be treated as though it were genuine. Action to be taken as the result of a bomb threat must be based on preplanning and the nature of the information received, as occurred at the Baldwin Area Medical Center in Wisconsin. The hospital administrator received a bomb threat on his direct telephone line. The caller said “bomb 20 minutes.” All nonessential personnel were evacuated from the facility; however, patients were kept in the hospital as well as necessary staff to care for them.<sup>5</sup> What made this threat somewhat unique was the specified time frame.

While most bomb threats are received by telephone, this is not always the case. In November 2008 the Sudbury Regional Hospital in Sudbury, Ontario, Canada, received a written bomb threat and decided to go public with the information for the first time although this was not the first time the hospital had received a bomb threat. Security officers were deployed to greet visitors with a prepared written script explaining the threat and that security had been heightened. All patients, staff, physicians, and volunteers were also advised of the situation. This allowed for various appointments and routines to be changed if necessary; however, the hospital continued to conduct business as usual.<sup>6</sup>

Bomb threats often are just that, a threat, but there can also be real bombs, as San Francisco General Hospital learned firsthand. In May 2007, a pipe bomb was found on the hospital’s loading dock. Then just 2 weeks later two more devices (wired and ready to detonate) were found on the perimeter of a campus building. Police and explosive experts were able to render this second round of devices inert without further incident.<sup>7</sup> In November 2008, Memorial Hospital of Union County in Marysville, Ohio, had to evacuate after a smoke bomb was thrown inside an entrance door. A second device was placed in a trash container near another entrance but with no damage.<sup>8</sup>

## Burglary

*The unlawful entry of a structure, with or without force, with the intent to commit a felony or larceny.*

The loss of assets does not always occur through theft and robbery. Burglary, too, is common in healthcare facilities. Although one might suspect that the hospital pharmacy would be a primary target, the advent of 24-hour pharmacies and the alarming of closed pharmacies have been instrumental in reducing the number of such burglaries. However, there are numerous other targets for burglary in a hospital. The operating room narcotics and anesthesia supply top the list. The operating room is generally well isolated and is usually closed at night. As with robbery, any place where cash is stored, whether in large or small amounts, is a frequent scene of a hospital burglary along with storerooms, work areas, and offices.

The physician's office and dental offices are also common burglary targets. Since very few drugs are kept in these areas the burglar is usually after money and computer equipment. In some cases expensive medical equipment is also taken. Optical shops have a high risk for burglary with eye glasses frames being the primary target.

Not all burglaries occur late at night or involve closed facilities. A phony repair person stole expensive parts from three sonogram machines at the University of Michigan Medical Center (UMC) in Ann Arbor, MI, at an estimated cost of between \$30,000 and \$45,000. The burglar arrived at the hospital's radiology department and began working on the equipment. He wore a uniform and informed staff he was a service representative. Later a staff member noted that he had not signed the maintenance log and he could not be located in the facility.<sup>9</sup>

Medical specific equipment and supplies found in healthcare facilities are not the only targets for burglaries. In late 2008, copper thieves struck Ben Taub Hospital in Houston, turning off the water to the toilets in a number of restrooms and stealing copper flush valves.<sup>10</sup>

Hospital parking areas are another frequent source of burglaries that deserve a high level of preventive security safeguards. Many healthcare facilities have seen a significant increase in the volume of auto thefts. A large health system in Phoenix, AZ, shared this was their greatest security risk as it was creating a high volume of employee turnover and negatively impacting patient satisfaction scores. The reasoning is unclear; however, local law enforcement officials suggested that the re-direction of funds to homeland security initiatives has required agencies to eliminate their auto-crime division. This redirection of funds has reduced the number of apprehensions and investigative efforts placed to prevent or respond to auto-related crimes.

## Dissident Group Actions

*A person, or persons, who differ in opinions or feeling with general refusal to conform to authority, sentiment, or policies of a majority.*

Major healthcare facilities have not experienced a great deal of disruption or damage related to demonstrations, civil disturbances, or sabotage in recent years. The abortion and animal rights issues are perhaps the current hot spots in this regard.

The numerous civil disturbances of the late 1960s and more recent Los Angeles riots are a reminder that healthcare facilities are not immune from incurring damage to facilities and injury to staff. Experience has shown that victims of dissident group actions are generally a mix of rioters, prisoners, bystanders, and public safety-type personnel. This mix of "players" creates a major challenge for the healthcare security administrator.

The list of security concerns to be managed during a civil disturbance varies, depending to a large extent on whether the hospital is located within the disturbance area or outside of it. Problems common to both situations include:

- The separation of rioters and riot control personnel while they are being treated.

- Strict visitor control, as injured rioters often are accompanied to the facility by friends or relatives who may wish to continue confrontational actions.
- An area-wide curfew, which can affect the reporting and releasing from duty of employees.
- The housing of personnel who cannot return home and people from the community who may seek refuge within the facility.

In addition to these common factors, a facility that is the target of civil disturbances or located within the area of the disturbance must deal with the following:

- Employees seeking access to a police-controlled area when attempting to report for work.
- Safety of arriving and discharged patients.
- Safety of personnel traveling within the controlled area.
- Sniper fire at or around the facility.
- Fires set within the facility.
- Fire bombs thrown into the facility or onto low roofs.
- Sabotage of the physical plant.
- The acquisition of additional supplies and equipment and the general need for increased housing.

Planning for civil disturbance activities can generally be viewed as an extension of the management of the security risks of the facilities identified in emergency management planning.

## Disturbances

*The actions of a person, or persons, to interfere with the normal tranquility and order of an environment.*

A continuing security risk is the disturbance or disorderly conduct incident. This type of incident can occur virtually anywhere within or outside the facility, including parking lots, employee locker rooms, lobbies, work areas, and patient rooms. Disturbances can involve patients, visitors, or staff. Many incidents of disturbance simply involve verbal arguments of varying degrees; however, these verbal arguments frequently lead to assault and the destruction of property. The number of disturbances taking place can often be correlated directly to the size, location, and type of facility. The type of patient, which relates to the type of visitor to some degree, must also be factored into the security plan for preventing and managing disturbances.

A common area for disturbances is the emergency/outpatient department. Large urban hospitals with busy emergency rooms can experience incidents on almost a daily basis. Many such facilities have found it necessary to station security personnel in the emergency area on a 24-hour basis. Patients who become combative in an emergency

room will usually be intoxicated, drug-impaired, mentally impaired, or forensic (police custody) patients.

The patient is not the only source of disturbances. Persons accompanying the patients are often involved. Many such incidents are precipitated by long waits for medical treatment, lack of information, or alleged improper treatment. Minor disagreements can end up with physical confrontation and property destruction. Such incidents can be averted if the caregiver staff informs the patient, or accompanying persons, of the reason for delayed treatment or the type of treatment to be rendered.

A particularly dangerous source of trouble is the person who comes to the health-care facility with the intention of engaging in a domestic confrontation with a spouse, boyfriend, girlfriend, or significant other. These incidents can lead to serious injuries, and the security officer can easily become injured in attempting to control these types of confrontations.

Another fairly common occurrence involves a visitor who is intoxicated, or under the influence of drugs, and demands to visit a patient. These persons can usually be talked down or escorted from the property before causing a disturbance. This type of incident often requires a show of force and must be handled very quickly to control an escalation of the problem.

## Drug Abuse

*The use of drugs to one's physical, emotional, and/or social detriment without being clinically addicted.*

A security risk that appears to be prevalent in recent years is that of drug abuse among healthcare employees. Although drug abuse is not unique to employees in the healthcare field, it is of great concern because patients may be placed in danger. Despite increased security measures, namely electronic dispensing systems such as Pyxis machines, and other unit dose systems, the theft of drugs from healthcare facilities continues to occur at extremely high levels. Healthcare facilities simply do not aggressively address this problem. A typical scenario can be found in the recent arrest of a surgical nurse at a Boulder, CO, hospital. According to reports, as many as 350 patients who underwent surgery within one 30-day period could have been denied the full amount of the painkiller drug Fentanyl. The nurse accessed the pain medication as often as 25 times in one day, replacing the drug with a saline solution by removing the vial's flip-top seal. It is, of course, no surprise that a hospital spokesman, following the arrest of the nurse, stated that the hospital's pharmacy had upgraded its system for monitoring drugs to flag any suspicious patterns.<sup>11</sup>

Theft of anesthesia-type drugs is so prevalent that at least two major teaching hospitals have announced a program of random drug testing of anesthesiologists. Both Massachusetts General Hospital and the Cleveland Clinic Foundation are now conducting random urine drug testing in their anesthesia residency teaching programs.

The Cleveland Clinic conducted a survey, in 2005, of anesthesiology residency programs and found that 80% of such programs reported problems with drug abuse. A total of 19% of these programs reported a death resulting from overdose.<sup>12</sup>

It is well known among healthcare security administrators that a great number of employees in healthcare facilities have purposely selected the facility with the intent of diverting drugs. Narcotics addiction among doctors and nurses is a much more serious problem than is generally recognized. The ease with which various caregivers can obtain narcotics contributes significantly to the problem.

## Embezzlement

*The misappropriation, misapplication, or illegal disposal of entrusted property with the intent to defraud the owner or beneficiary.*

The healthcare setting presents an environment with a host of opportunities for the crime of embezzlement to occur. The proliferation of electronic transfer of funds by individuals and third-party payers has reduced the opportunity for large-scale funds loss due to embezzlement. Nevertheless, there remains ample opportunity to commit this type of crime. There is money changing hands in cafeterias, gift shops, cashiers, registration areas, and the handling of petty cash accounts throughout daily operations in our healthcare facilities.

## Fire/Explosion

*The ignition of combustible materials.*

Arson is a security risk which can have grave consequences not only in property damage but human suffering as well. Incidents involving arson do occur in healthcare facilities. The disgruntled employee, or ex-employee, is often responsible for these acts. Labor disputes sometimes spawn this type of act and organizations should be especially aware during these times. Areas that require close attention are storerooms, employee locker rooms, lounge areas, equipment rooms, linen storage areas, loading docks, and especially employee and public washrooms.

## Hostage Taking

*A person held by a party as security that specified terms (demands) will be met by the opposing party.*

Healthcare organizations have experienced a relatively high number of hostage-taking incidents. These incidents have been most prevalent in the emergency department setting; however, physician offices, administrative offices, clinics, and pharmacies have not been immune to such incidents. While hospital staff have been the primary victims of healthcare hostage incidents, visitors and patients can also be victims. At Provena Morey Medical Center in Aurora, IL, police shot and killed a patient, armed with a gun, after a

4-hour standoff. The perpetrator had held another patient as a hostage but released him during the standoff. The perpetrator came out of a room allegedly pointing a gun at police at which time he was shot and killed.<sup>13</sup>

Other major hostage-taking incidents within healthcare facilities include such headlines as:

- “Hospital Held Hostage” in Sandy, UT. A gunman held patients, staff, and infants hostage for 13 hours in which he threatened to set off a bomb and a nurse was killed.
- Eight staff and a patient were held hostage in a Boston, MA, hospital emergency room for over 90 minutes by a gunman who entered the hospital as he was being chased by police. A doctor, nurse, and a housekeeping employee were able to wrestle the gun from the gunman bringing the incident to an end.

## Homicide

*Killing of one person by another.*

Healthcare organizations experience frequent incidents of homicide. These incidents involve practically all the different categories of stakeholders in the medical care environment as both victims and perpetrators.

The motives for homicide incidents involve intimate personal relationships, angered patients, disgruntled staff and visitors, prisoner patient escape attempts as well as mercy killings by staff and loved ones. Of particular note relative to homicides in the healthcare environment is that the motive is quite frequently an issue over alleged poor medical treatment. In this regard, there can be a rather long time period between the alleged care and the actual act of retaliation.

In Columbus, GA, an armed man shot and killed a nurse, administrative assistant, and bystander. The assailant had apparently held a grudge for over 3 years since the death of his mother who had been treated in the hospital before she died of natural causes. The gunman believed a specific nurse, the one who was killed, had not properly taken care of his mother while she was in the hospital. After the shooting, a plain clothes police officer shot the gunman who was then taken into custody to face murder and assault charges.<sup>14</sup>

In 2006, Derrick McFarland, a security officer at Montgomery Regional Hospital in Blacksburg, VA, was killed by a prisoner as he escaped from custody while being treated at the healthcare facility. The prisoner, William Morva, overpowered a sheriff's deputy assigned to watch over him when he was able to overtake the deputy and his gun. Once in the hallway, he came across officer McFarland and shot him through a glass hallway. Morva had been a patient in the facility for over a year and was not considered an out-of-the-ordinary security risk.<sup>15</sup>

A gunman opened fire at a Monroe County, NC, nursing home and killed eight people, including seven elderly residents and a nurse, and wounded three others. The motive of the gunman is unclear, but authorities believe Robert Stewart was attempting to kill his estranged wife, who worked at the nursing home. She was not among those killed.<sup>16</sup>

Mercy killing of patients in the hospital are often carried out by a spouse or “loved one.” Multiple killings have also been committed by caregivers throughout the course of history of medical caregiving. A case in point is one Charles Cullen, a nurse, who has been charged with murder after confessing to killing 30–40 patients in Pennsylvania and New Jersey between 1987 and 2003, by injecting them with drugs. During this time, Cullen worked in some 10 different medical care facilities.<sup>17</sup>

Even gangland-type homicides occur in medical care facilities. Early in a predawn morning five masked and gloved gunmen entered the Louis Hospital, St. Croix, in the Virgin Islands. They forced their way into the third floor surgical unit. The gunmen then emptied their magazines, sending dozens of bullets into a patient. It took the gunmen only a few minutes to enter the unit, murder the patient, and flee. The victim in this case was one of two prisoners in the custody of the Bureau of Corrections. There was only one armed corrections officer guarding the two patients. The corrections officer was in the room of the other prisoner at the time of the shooting.<sup>18</sup>

## Identity Theft

*Identity theft occurs when someone else uses another person's identifying information (e.g., name, social security number, credit card number, etc.) without permission, to commit fraud or other crimes.*

It is estimated by the Federal Trade Commission (FTC) that as many as 9 million Americans have their identity stolen each year. While some identity theft victims can resolve their problems quickly, others are required to spend large sums of money and time repairing the damage to their name and credit record. Victims may lose out on job opportunities, be denied loans, and in some cases may even be arrested for crimes they did not commit.

The healthcare setting can be a lucrative setting for the identity thief. The public access to offices, clinics, treatment areas, cafeterias, and patient rooms can be good “hunting grounds” for the purse and the wallet left unprotected. The use of credit cards and records maintained during the normal course of providing patient care can also lead to identity theft by staff.

The three stages of identity theft are: *acquisition* of identity information, *use* of the information, and *discovery* of loss. The longer it takes to discover the theft, the greater the loss incurred and the diminished the chances for a successful prosecution. Older persons and those who are receiving inpatient or outpatient medical treatment are at high risk of being an identity theft victim.

The US Federal Trade Commission estimates that 250,000 Americans had their medical identity stolen or misused in the past few years and the problem is growing. This growing problem is due, in part, to providers of healthcare shifting to greater utilization of electronic records. Medical identity theft victims are at risk of being denied medical care and have few options in restoring their medical records, especially given the privacy restrictions of recent government regulations.



## Imposters

*One who engages in deception under an assumed name or identity.*

The imposter represents another security vulnerability that occurs with a high degree of frequency. The Certified Nurse Assistant (CNA) or licensed practical nurse (LPN) who has fraudulent identification indicating the status of a registered nurse (RN) appears in all segments of the healthcare industry. There have been numerous accounts of people who claimed to be physicians, visited patients, gave care, and interacted in their assumed role for considerable lengths of time before their false identity was discovered.

In Ohio, a man impersonated a physician for over 4 years until his true identity was discovered by a “patient” he had treated. The patient was a police officer who, after knowing the imposter for a number of years, became suspicious. Subsequent investigation resulted in the arrest of the physician imposter but not before he had treated individuals, utilizing space, supplies, and equipment from several Cincinnati hospitals.

In the 2-week period from February 26, 2005, to March 3, 2005, there were three reported cases of imposters entering hospitals in Los Angeles, Boston, and Detroit. There were similarities in these three incidents including physical descriptions of the persons, posing as TJC surveyors, questions asked, and time frames. TJC officials verified that no surveys of those hospitals had been scheduled at those times.<sup>19</sup> Just a few weeks later an unidentified man attempted to gain access to three Indiana hospitals. The FBI was notified in these cases and conducted an investigation.<sup>20</sup>

An imposter at two South Florida hospitals was able to create a nightmare of sorts for two hospital security directors and four police officers. The imposter claimed to be a physician and while wandering corridors, demanded to be treated as a VIP. The tables were turned, however, as the imposter obtained a restraining order against the police and security which formed the basis for the removing of weapons and gun permits requiring a court appearance.<sup>21</sup>

## Kickbacks/Fraud

*Kickback – Money or something of value given to an employee of an organization by a vendor or contractor in exchange for a consideration.*

*Fraud – An element of an offense consisting of deceit or intentional misrepresentation with the objective of illegally depriving an entity of the owner's property or legal rights.*

As organizations grow, the risk of kickbacks to well-placed staff members also grows. As the dollar amount of contracts, purchases, and construction grows so does the potential for kickbacks. Proving that a person is guilty of accepting a kickback can sometimes be difficult to accomplish. In many of the kickback scenarios there are only two persons with knowledge of the crime and both parties have realized a financial gain. The size,

complexity, number of financial transactions, and big dollar expenditures make health-care organizations at high risk for kickback situations to occur.

Healthcare organizations are at high risk for vendor fraud perpetrated by employees due to the high number of miscellaneous supplies ordered. A typical method of vendor fraud is for an employee to create a small shell company. The employee then forges a billing to the employer and approves paying organizational funds to the shell company. Signs that should alert organizations to vendor fraud include a post office box address especially in a nearby zip code, an email address from a for-fee Internet provider (e.g., Yahoo, Comcast, and MSN), and missing information in any vendor-data records.<sup>22</sup>

The cost of fraud to individual healthcare provider organizations is insignificant, however, when contrasted to Medicare/Medicaid losses which are multi-billions of dollars a year. The extent of this fraud is so extensive that any meaningful projections are difficult or impossible to calculate.

## Kidnapping/Abduction

*A kidnapping or abduction takes place when a person is detained or taken away by using threat or physical force.*

Virtually all healthcare provider organizations, and the general public, are aware of the risk of infant abductions from hospitals and other birthing centers. The risk of infant/pediatric abductions can be viewed as either an abduction by a nonfamily member (stranger) or an abduction by a family member (domestic). It is the stranger-to-stranger abduction that is the most problematic for the healthcare organization.

The National Center for Missing and Exploited Children in partnership with Mead Johnson Nutrition has produced an educational program entitled “Safeguard Their Tomorrows.” This program is directed primarily to healthcare professionals involved with birthing and pediatric care. It has been presented to over 64,000 healthcare and public safety personnel in the United States and Canada since its inception over 20 years ago. The program, updated several times, is credited to a large extent with reducing a significant number of nonfamily abductions. The prevention of and response to infant and pediatric abductions from healthcare facilities are treated more fully in *Chapter 20, Security Sensitive Areas*.

## Labor Actions

*A labor action, in the context of security, is an activity that is designed to interrupt or cause a financial burden on an organization by a labor organization.*

In 1974, healthcare employees came under the jurisdiction of the National Labor Relations Act. The Act gives employees the right to collective bargaining representation. In order to preclude interference with patient care during the process of unionization, the National Labor Board defines what groups are eligible for bargaining representation.

It should be noted that the law generally provides that an employer is not obligated to recognize a union for security personnel at a specific healthcare facility if the proposed union represents any other employee group at the facility.

Labor disputes can create a myriad of protection problems including threats, harassment, destruction and damage to property, intimidation, sabotage, and injury to both the innocent person and the person who is either represented by a union, seeks representation, or is simply sympathetic to the organized labor cause.

Protection problems encountered during a strike are somewhat similar to those to be managed during a civil disturbance. These problems include the following:

- The disruption of services from within.
- The disruption of external services, such as deliveries and trash removal.
- Malicious destruction of facility-owned property and the personal property of employees, such as parked vehicles.
- Intimidation and assault of promanagement employees.
- Harassment in general, such as illegal secondary boycotts.
- Altercations between pro-union and anti-union persons.

## Loss of Information

*The loss of information critical to the mission of the organization or information of others entrusted to the organization.*

The theft and/or misuse of confidential information, or privileged information, are security risks that are often overlooked in medical clinics and hospitals. Of primary importance are the medical records of the patient. These records often contain valuable information concerning lawsuits and other legal action. The methods of stealing information have changed radically over the years with the advent of electronic transfer and storage of healthcare records and reports. A whole new industry regarding the protection of critical information has evolved and has been termed *enterprise management*. Loss of information can occur as the result of theft of computer hardware, unauthorized access, unsecured networks, and inadequate security for database files. The growing use of the telehealth/telemedicine systems by healthcare providers has created a whole new opportunity for the compromise of information. Other types of proprietary data that must be properly safeguarded include incident reports, bid specifications, certain financial records, and legal documents.

## Patient Elopement

*A patient who may be incapable of adequately protecting himself or herself who departs the healthcare facility without the knowledge and agreement of clinical staff; also referred to in some countries as absconding.*

Healthcare providers assume a high degree of responsibility for the safety and welfare of patients whether they are inpatients or outpatients. Maintaining an accountability of their whereabouts during treatment varies to a degree depending on the type of patient. There is, of course, a high expectation in terms of this accountability regarding the mental health patient and the pediatric patient. The patient who simply leaves during the treatment process without the knowledge of a caregiver is an incident that is generally referred to as an *elopement*. In simple terms, the patient has left the facility either by rational decision or due to impaired mental capacity. In the latter case, the patient is subject to great injury or even death in terms of weather, accidents, or failing to take life-saving medication/treatment. In late 2008, University of Pittsburgh Medical Center had an 89-year-old dementia patient who wandered away from her 12th floor room to be found a day later dead on the roof of the hospital. The hospital said in a public release statement that they would strengthen their procedures to search for missing patients to include use of monitoring devices and possibly search dogs.<sup>23</sup>

## Robbery

*The unlawful taking or attempted taking of property that is in the immediate possession of another by force or threat of force.*

Armed robbery within healthcare facilities and on the grounds is a continuing security problem. A main threat to a medical center involves the pharmacy, which routinely stocks large quantities of desired narcotics and other dangerous drugs. While neighborhood pharmacies face the threat of an armed robbery, it is generally the result of seeking cash as opposed to drugs. Although most drug-related armed robberies in the medical center involve the pharmacy, there have also been reports of robberies occurring in the emergency room and even at nursing stations. A nurse leaving for a smoke break at a southern Colorado hospital was brusquely met at gunpoint at the emergency exit and forced to re-enter the facility and access the narcotic dispensary where the armed assailant took a large amount of narcotics and left the facility without further incident.

In addition to drugs, another target of armed robbery is cash. The main cashier is a likely target, but robberies of cafeterias, gift shops, outpatient cashiers, parking lot cashiers, and other areas where cash is handled or stored have occurred. The robber's timing, however, is not always right. In one case two armed people held up a cafeteria cashier at 3:30 P.M. and escaped with less than \$20. Just minutes before, the breakfast and lunch cashier had cashed out the register drawer for the afternoon cashier to take over.

Robbery is also of major concern on medical center grounds. Victims are often visitors, which can lead to negative public relations for the organization. The hospital inpatient can become very upset, especially if the victim is a spouse who was on the way home from visiting the patient. Other patients quickly learn of the incident, and word spreads to relatives and friends. Thus the healthcare organization becomes a secondary victim to the robbery resulting with collateral damage.

## Stalking

*Stalking is to pursue by tracking stealthily.*

The healthcare environment provides many opportunities for the stalker to operate. A stalker is one who tracks his victim and generally attempts to make unwanted personal contact. While the contacts are usually in person, the stalker will sometimes pursue his victim through telephone calls, faxes, letters, or electronic mail; stalking can be a precursor to escalating threats and physical confrontation. Researchers report an estimated 1,006,970 women are stalked each year compared to 370,992 males.<sup>24</sup> The high number of female staff and the openness of medical center campuses results in a high number of stalking incidents. Most stalking problems are based on a previous relationship of the two persons. However, there are cases of a stranger-to-stranger situation. In the case of the latter, the victim is often a well-known personality in the community. As with bomb threats, each reported stalking incident must be taken seriously and it is an area where considerable proactive preventive steps can be taken. A common proactive step is the obtainment of a restraining order; however, in a survey it was reported that 80% of these decrees were violated.

## Terrorism

*The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments.*

The terrorist act is a risk that is actually a combination of other risks, including fire, bomb, bomb threats, destruction of property, and kidnapping (hostage taking). It is, however, considered a separate risk due to the distinct motive that precipitates the act. As in strikes and civil disturbances, the primary safeguards to be applied are the expansion of the everyday protection elements in place, e.g., increased security personnel, greater facility restricted access, increased staff awareness, and attention to good everyday security practices. There continues to be serious debate among healthcare security practitioners as to the level of risk to healthcare facilities by terrorist action. In general, the consensus of opinion is that healthcare facilities are at relatively low risk; however, a terrorist act in the geographical area of a healthcare facility can produce a high level of collateral damage.

A familiar tool for domestic and international terrorists, bombs have been used to execute some of the world's most devious and radical acts of terrorism, such as the Madrid, Spain, train station bombings in 2005. As critical infrastructures serving important community roles, hospitals specifically must take the risk of terrorism with great seriousness and not underestimate the potential for harm and significant organizational disruption.

## Theft

*Theft is the act of larceny, often referred to as stealing.*

The pilferage or theft of supplies, equipment, and personal property is a reality for all healthcare organizations. There are many estimates of the extent of theft in hospitals as there are estimators. A generally accepted estimate of loss for US hospitals by industry experts is between \$7,000 and \$8,000 per bed per year. In terms of losses for all healthcare organizations a conservative estimate projects a cost exceeding \$50 billion on an annual basis.

It is virtually impossible to calculate the specific losses of any single facility. Like an iceberg, only a small part of the problem actually surfaces and it is often difficult to properly attribute the loss to theft, waste, or loss of accountability. In the opinion of knowledgeable administrators, however, loss is a substantial item in the cost of operating any medical care facility, regardless of size or location. Because more than 3,000 items purchased by healthcare facilities are usable in the home, the list of items being taken from hospitals is quite lengthy. Items that top the list are drugs, linens, food supplies, medical equipment, and maintenance parts and materials.

A pathologist and three other people were charged with the illegal sale of human organs, tissues, and fluids, which were in the custody of a Veterans Administration Hospital in California. These parts of the body, removed during autopsies, were sold to biomedical companies. Biomedical firms use human organs and fluids to do research and develop diagnostic tests.

A recent series of equipment thefts from Florida hospitals indicates how large amounts of expensive medical equipment can be stolen in a short time. The Florida Hospital Association reports that from October 1997 to mid-October 1998 there were medical equipment thefts from 48 different hospitals and some hospitals reported more than one incident. These known thefts totaled nearly \$2.5 million. Primary items being stolen were cardiac monitors, pulse oximeters, life pack defibrillators, endoscopy, anesthesia machines, and even c-arm fluoroscopic units.<sup>25</sup>

A disturbing trend is the theft of sharps containers. Often used for the wasting of fentanyl patches and other syringes filled with narcotics, thieves have targeted these boxes, ripping them off the wall. Not as common is the theft of pain pumps (drug administering machines), but two hospitals in metropolitan Denver, CO, have had a drug-seeker steal the device and the schedule II narcotics they were dispensing directly from the patient room while in use.

## Employee Theft

Security practitioners agree that the majority of healthcare organization losses from theft can be attributed to employees. The employee thief works every day, creating a constant drain on resources, as opposed to people from outside the organization who generally do not have recurring opportunities to steal. Numerous ingenious employee theft schemes have been revealed; however, the biggest loss comes from the magnitude of employees who simply dip into supplies with only a slight chance of being caught.

Although the data were collected some 25 years ago, the most in-depth research into employee theft in hospitals was conducted by the Sociology Department at the University of Minnesota under a Law Enforcement Assistance Administration grant.<sup>26</sup>

A total of 37% of hospital employees who responded to the survey in this study indicated that they had been involved in taking hospital supplies. Of these, 11% admitted engaging in the theft of supplies on a monthly or more frequent basis.

In addition to the theft of general supplies, the study revealed several other areas of interest to the hospital security administrator.

Took tools or equipment	8%
Received excess expense reimbursement	2%
Was paid for more time than worked	9%
Took or used hospital medications	10%

Study findings were based on questionnaires sent to a cross-section of employees. The number of employees revealing misdeeds was high; however, the actual number of thieves was undoubtedly much higher than was admitted. Some respondents were unsure if the document could not be traced back to them, even though the study process was completely anonymous. In addition, most people know right from wrong and tend to deny any wrongdoing as a matter of course. These two factors alone would certainly account for some understating of the magnitude of the problem.

#### *Factors in Employee Theft*

An objective of the Minnesota study was to determine the circumstances under which employee theft was most likely to occur. Although the study did not focus on counterproductive behavior, its incidence appears to have a direct correlation to theft. The employees who reported above-average theft levels were also quite prone to above-average counterproductive behavior, such as taking extra long lunch and coffee breaks, working slowly or poorly, using drugs or alcohol at work, and abusing sick leave.

The study concluded that the younger and never-married employees have a high level of theft involvement. An explanation for this is that they are less vulnerable to management sanctions, including dismissal, because they have no dependents and generally a low seniority status.

Job dissatisfaction also leads to higher theft involvement, especially in the younger work force. The most consistent source of employee dissatisfaction was found to be in the employee-supervisor relationship. The study also concluded that employees who frequently got together with co-workers after hours were involved in a higher level of theft activity.

The most consistent predictor of theft involvement found by the study was the employee's perceived chance of being caught with the potential of being fired or arrested. When there was a visible and strong opposition to theft on the part of management and

co-workers, the amount of theft decreased. It is of interest that the inferred sanctions imposed by co-workers appear to have had a much stronger influence in shaping anti-theft behavior than did the more formal action of management.

#### *Effects of Controls on Employee Theft*

Another important goal of the Minnesota study was to determine how effective certain actions or controls imposed by the organization were on reducing the amount of employee theft. The controls reviewed were the security department, management policy, inventory, financial procedures, and pre-employment screening.

The study indicated that the level of sophistication of a security department has little effect on theft reduction. This is not surprising as the major thrust of the majority of security operations reviewed addressed the problem of external theft control, grounds safety, employee safety, and other nonemployee theft-related activities.

As one would expect, clearly defined theft policies, inventory programs geared to detecting losses, and the effective pre-employment screening of job applicants all tend to lower the level of theft in an organization.

#### *Reporting Healthcare Facility Property Losses*

It is extremely difficult to develop a program of theft control unless the extent of the problem can be measured. One method of measurement is a good reporting system that requires all employees to promptly report missing property. It is in this area, however, that healthcare organizations have failed miserably. It is estimated that the healthcare security departments receive reports on facility property losses in only 1% or 2% of cases. The chief reason for poor reporting is that the supply lines are so open that stocks are quickly replenished as ordered. In addition, employees do not want to get involved, especially when facility management does not seem to care. Property losses can also be viewed as supervisory failures, and thus, staff at all levels tend to ignore the problem.

#### *Patient Property Losses*

Theft and loss of patient property is a continual concern for all healthcare provider organizations. Although the value of missing patient property is minimal when compared to the loss of facility property, most organizations place more emphasis and more effort on protecting patient property and investigating patient losses than they do on protecting their own assets. Missing patient property can seriously affect public relations, and the patient can interpret this problem as an indication that the medical care may also be inferior. In some instances patients become so upset over a theft of their property that their medical condition is adversely affected.

The healthcare employee is not always responsible for patient property losses. In one case a patient in a nursing home could not locate his false teeth. Investigators solved the case when the teeth were discovered in the mouth of another patient.

One of the serious questions facing an organization when a loss is reported is whether the matter is one of accountability or actual loss. Many patient belongings are



reported stolen when in actuality the property has been misplaced, accidentally discarded, or taken home by a family member or friend.

In such cases where property has unknowingly been taken home the claim of theft is usually made in good faith, and most patients advise the hospital if the item is found. Some patients, however, rationalize that since the hospital thinks something was stolen, it might reimburse them for the loss. It is not uncommon for these patients to feel that they deserve anything the hospital pays them because they are paying extremely high hospital charges. Other patients may be embarrassed that they caused trouble over nothing and thus hesitate to inform the hospital that the lost item has been found as opposed to being stolen.

The question of responsibility or liability is usually raised in the investigation of a loss that is not successfully recovered. Laws vary, of course, but the healthcare organization generally cannot be held responsible for all property brought into the facility by a patient or visitor. The organization must take every reasonable precaution to see that the patient's property is safeguarded so that losses do not occur, but it is generally accepted that any loss is the responsibility of the patient and that the organizations should not automatically reimburse patients for losses.

An exception exists where the facility has a valuables protection system. In such a system, where the patient has actually been given a receipt for the property and the property is subsequently controlled by the facility, the organization would, of course, be liable for any loss.

A complicating factor concerning patient property is that the property in the custody of the patient is not constant. Patients rarely go home with the same property they had when they checked in to the care facility. Visitors often bring gifts, and the patient often requests that additional items be brought to the facility by relatives or friends. Thus the property belonging to, and in control of the patient, is in a constant state of change.

### *Employee Property Losses*

The loss of employee property is another problem that confronts virtually all hospitals, clinics, and long-term care facilities. This risk can generally be correlated to the size of the organization. In a large facility, the anonymity factor and the erosion of interpersonal relationships combine to create an environment that tends to increase the theft of employee property. This does not imply that larger organizations necessarily have more theft. The application of security safeguards can effectively manage this risk, resulting in a good record of theft prevention for any facility if administration is seriously concerned with the proper management of this risk.

The most common loss among employees is the purse left on an open shelf at a nursing station or under an office desk. Other commonly stolen items include shoes and articles of clothing. Although theft can occur at any time, experience shows that it can sometimes be predictable. A prime example is the theft of winter coats and vehicle batteries in places that have fairly severe winters. There is generally a rash of these thefts at the onset of the winter season, and they taper off as the thieves get what they need to see them through the winter. The holiday seasons also provide more opportunities for theft.

As with patient property, the dollar value of employee property losses is quite low compared to organizational losses. Regardless of dollar amounts, however, employee property loss is often a key factor in employee relations. No one wants to work in a facility where losses, distrust, and suspicion are ongoing problems. In contrast to the extremely low reporting level of hospital property losses, it is estimated that security receives reports on up to 95% of all employee property losses.

## Security-Related Risks

There are risks facing healthcare organizations that often receive attention as security issues but are not directly related to the security program. These security-related issues are actually more clinically related and should be managed and controlled within the operating department. The security function may play a supporting role; however, the ownership of the risk does not reside with security. Two good examples of these security-related risks would be in the misuse of medical record information and the infrequent but serious problem of infant switching or discharge to the wrong family. Healthcare providers have a responsibility to protect patient medical information from loss, misuse, and the compromising of confidentiality. This responsibility rests with the functional department in possession of the information as well as with the information systems department. The growing use of electronic patient information systems mandates that the whole area of computer access be addressed. Nursing units must protect their point of contact information and the medical records department must guard against theft and improper release of information.

The baby switching or wrongful discharge problem is one of providing proper clinical management within the specific medical care unit. The protocols of infant identification, staff and mother education, and compliance with established policy and procedure rest squarely with the operating unit. These mix-ups can go undetected for many years as was the case at a medical center in Virginia. In 1998 it was discovered that an infant switch had taken place over 3 years earlier. In 1999 a Southern California hospital discovered a baby mix-up within several hours of the occurrence. One infant had been discharged with the wrong parents. The second infant was still in the hospital and the error was corrected quickly through blood antibody testing.

## Safety-Related Risks

Among the safety-related risks that affect the protection level of the organization and relate directly to the security program are accidents, fires, and disasters.

### *Accidents*

All facilities must be concerned with employee, visitor, and patient safety. Safety in this regard refers principally to preventing injury caused by unsafe physical conditions or the inadvertent act of the victim or another person.

It is somewhat paradoxical that the safety record of some healthcare facilities is inferior to those of the major industries that send accident victims to them for care.

Because they treat a wide variety of accident cases, hospitals should have a special awareness of the need to maintain an adequate safety program. Many of the accidents involving healthcare employees are similar in nature to those occurring in industry, although the major problem of needle sticks is somewhat unique to the healthcare working environment.

The courts have consistently ruled that all medical care facilities are required to maintain safe premises and patient safety is a major focus of TJC. The costs of medical care, loss of services, malpractice and public insurance liability, loss of materials and equipment, human suffering, and loss of public goodwill are just some of the reasons why medical care facilities must constantly guard against accidents.

#### *Fires (Accidental)*

Fires in medical care facilities can contribute to a high loss of life and property. The incidents of accidental fires and explosions in healthcare facilities have been reduced over the past years. This reduction in the number of fires, and certainly in their severity, has been due to, in large part, TJC standards and local fire department fire prevention efforts. The issue of accidental fires and explosions clearly falls within the safety function with a good deal of support from security. Fires caused by smoking have been significantly reduced through stringent smoking restrictions in healthcare facilities.

#### *Internal and External Emergencies (Disasters)*

Security concerns during an external disaster center around controlling visitors, safekeeping patient valuables, controlling external traffic of pedestrians and vehicles, providing extra security support to the treatment areas, and designating an area for the dissemination of information concerning the injured. As disasters strike, new and often unanticipated factors present themselves to challenge even the most comprehensive and well-developed disaster plans. The major responsibility for managing the disaster-type risk is in the organization's emergency management function.

## Facility Security Risk Assessment

The identification of specific risks generally begins with a facility security review process. The identification and magnitude of security threats or risks, along with their potential impact on the healthcare organization, are but initial steps in protecting the organization. The objective of the security assessment/analysis is to identify the security exposures so that a comprehensive, effective, and cost-justified security plan can be developed and implemented. Analysis and evaluation of the risks provides the rationale that security measures (safeguards) are implemented appropriately based on protecting critical resources while accepting a calculated degree of risk. It is understood that an asset cannot be protected completely without extravagant cost or unduly inhibiting the primary mission of providing efficient and quality patient care. The goal of implementing countermeasures for security risks is to make it difficult for a security breach to occur—to harden

the facility as target. The level of difficulty to be implemented depends on the value of the asset and the organization's tolerance for risk.

When embarking on the process of a security risk assessment it is important to keep in mind the subtle differences between a risk assessment, security survey, security program review, and a security audit. The assessment is conducted to identify and evaluate security risk by the level of protective measures (safeguards) in place to manage an expectable level of risk. A survey is a more random evaluation of the overall program to determine the completeness, acceptance, strengths, and weaknesses in the program. The review is much the same as the survey; however, it will often focus on a specific area of security such as the emergency department, mother–infant unit, or change in space design. The audit is rather narrow in focus to determine the validity and operational aspects of a specific element of the security program. The audit is to determine if a defined element of the security system is operating in the manner intended and producing the end result as expected. In security we most often refer to this term relative to a review of a procedure to determine the degree of compliance with the procedure process and the need to make appropriate changes for identifying the need for training. Rarely does security become involved in the financial types of audits except in connection with an investigation.

### Who Should Do a Facility Security Risk Assessment?

A basic question that must be answered is: Who should conduct the assessment? As one might expect, there are several approaches. The first approach is to delegate this task to the person who is responsible for the day-to-day security program. An advantage of this approach is that the individual already possesses a general knowledge of the environment, including past problems, community assessment in terms of criminal activity, organizational philosophy, and organizational structure. This person most likely has good access to department heads and supervisors, all of whom may be more candid in their discussion of operational procedures and problems than they would be with a person from outside the organization. The main concern with the in-house approach pertains to the qualifications of the individual. The mere fact of being in a position does not in itself qualify a person to conduct a valid security risk assessment. A qualified person conducting a healthcare security risk assessment should possess a certain level of education and experience often validated by various trade association credentials. Experience in security, safety, or risk management in more than one healthcare provider organization is also a general requirement. The person should possess the designation of a Certified Healthcare Protection Administrator (CHPA) conferred by the International Association for Hospital Security and Safety or that of a Certified Protection Professional (CPP) conferred by the Professional Certification Board of ASIS International. Lacking one, or both of these credentials, can be compensated by involving a person with these credentials as part of the assessment process.

The second approach to who should conduct the security assessment is to use an outside consultant. The major advantage of this approach is that the consultant can be

more objective. The consultant can generally perform the assessment task in much less time than the insider and can bring a broad range of varied operational experience to the assessment process. In other words, the consultant does not need to find solutions from scratch and does not have personality conflicts with the facility staff or preconceived opinions regarding the organization. Internal politics and staff personalities can be avoided or at least mitigated through the consultant approach. The primary downfall is the costs of the consultant.

The third assessment method involves using a person from within the organization and an outside consultant. This method can combine the advantages of the other two approaches. The consultant selected to “co-conduct” the assessment must be familiar with the healthcare delivery process, knowledgeable of security issues surrounding the healthcare environment, and have security experience obtained from a variety of healthcare facilities.

Regardless of who does the assessment, employees often view the process as an investigation rather than being a nonthreatening business management review. The healthcare administrator must use every avenue available to communicate to stakeholders the objective of the review process. The objective is to assist departments in the performance of their specific function contributing in a positive manner to the overall mission and security of the organization.

## How Detailed Should the Assessment Be?

There are a great many methodologies and formats that can be utilized to assess security risks and to measure the severity of those risks. There are two basic principles to keep in mind regarding security risk assessments. The methodology should not be overly complicated and the bottom line is that risk-level conclusions are largely subjective in nature in terms of probability. The second principle is that a formal security risk assessment, conducted on a periodic basis, is simply a baseline that can and should be modified on an ongoing basis. Virtually every security incident provides an opportunity for lessons learned which may affect the assessment. Changing neighborhood dynamics and renovation and construction projects are also among activities that may have a bearing on the security risk analysis. Additionally, new and modified patient care programs including changing space allocations are important to consider.

The tendency to group all security assessments into a single category should be avoided. Not all assessments are intended to examine every facet of the entire healthcare facility. Many security risk assessments are conducted for a specific department or function as circumstances dictate.

A security risk assessment must be viewed in terms of the depth of the review process. A security risk assessment can consist of a general review or an in-depth department by department and function by function assessment.

The International Association for Security and Safety has developed a Basic Industry Guideline relative to healthcare security risk assessments. The association also has a “Risk

Assessment Toolkit” available which describes an in-depth approach to this important aspect of security risk management.

## What the Security Risk Assessment Should Include

A general security risk assessment of a healthcare facility need not be overly structured. There are no ready-made checklists that fit every organization. Keep in mind that every facility is unique. Checklists and guidelines are only resources that may assist in the review process. Just as there are no set guidelines on what should be reviewed, there is no exact starting point. The assessment should review the physical facilities and the major functions of the organization.

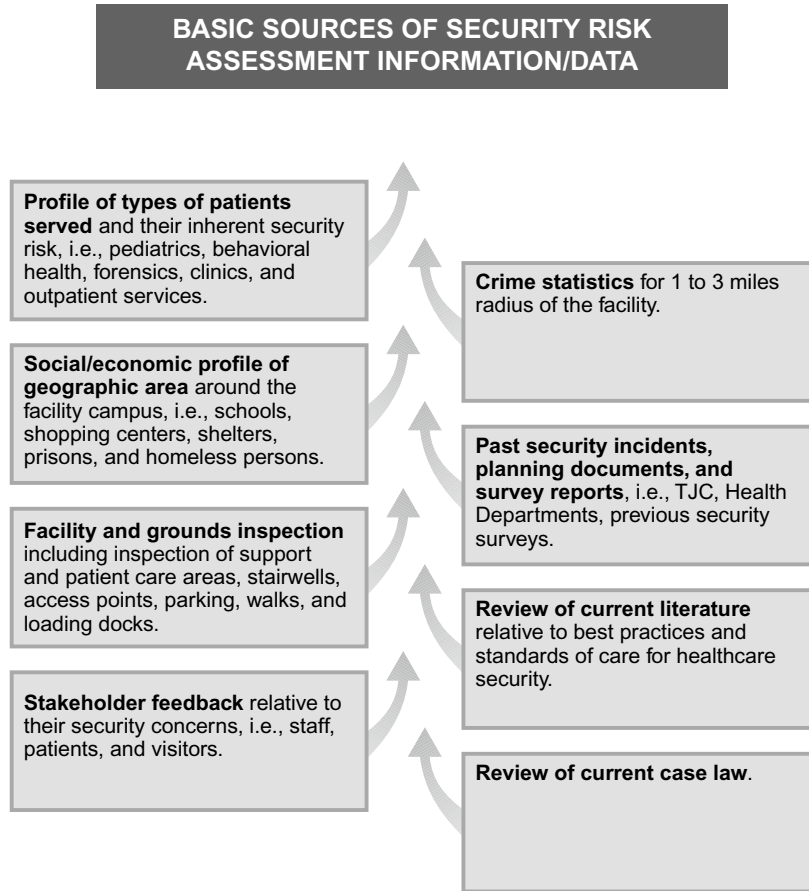
A good place to begin is with the physical facilities on the extreme perimeters of the property. Security can be referred to as a *system of perimeters*. In this concept the application of security safeguards becomes more strict or stringent as one advances to the interior. A simplified example of this concept is the protection of a hospital’s main narcotic supply. The grounds may be fenced; there may be limited traffic control, well-trimmed shrubs, and night lighting. Next is the building in which the pharmacy is located. This perimeter will be protected by walls, doors and locks, window protection, limited access control, and various security measures. Next is the pharmacy area, which will again be protected by walls, doors, and locks, window protection if required, as well as good department access control including alarm systems and closed circuit television. The final perimeter may be the safe, vault, or electronic dispensing system within the pharmacy itself.

## Assessing Risk

Each of the security risks identified must be assessed in terms of the degree of threat (real, perceived, and potential) to the organization. In rendering this assessment basic sources of information should be utilized. These information sources are shown in [Figure 3-2](#).

Analyzing risk in terms of real or perceived threat is more easily addressed than in terms of potential threat. Environmental criminology is the study of the spatial patterns of wrongdoing, perceptions, and space awareness of the criminal, criminal mobility patterns, target selection, and the decision to commit a crime. Although these factors pertain more directly to crime outside the organization, they do relate to varying degrees of internal crime and other negative acts.<sup>27</sup>

In addition to the foregoing, the legal implications of *foreseeability* must be taken into consideration. The courts consistently take the position of “totality of circumstances,” as opposed to the strict view of whether a similar incident previously occurred that would put the organization on notice. Such notice can go far beyond the organization’s property to include situations or incidents occurring down the street or across the nation. The best example of being on national notice is the vulnerability of infant kidnapping from hospitals. It would be very difficult for any hospital to defend itself on the premises that it was not knowledgeable that this type of event could occur.



**FIGURE 3-2** Security risk assessment information/data.

The whole area of a foreseeable criminal act relates directly to the probability of crime. Predicting the probability of crime for any given address principally in the United States and Canada is the business of CAP Index headquarters in Eaton, PA. The CAP Index company produces a variety of reports that are widely accepted by security professionals as part of the risk assessment process. The basic CAP Index report/map utilizes some 21 demographic variables, which are weighted, from updated census tract data, to predict crime probability for a specific address. The report/map produces a numerical score of crime probability for the address and compares the score to the national, state, and county averages. Also provided in the report are comparison scores, a past time period, current date, and a projected date. The CAP Index report can be ordered for a given date in the past and is frequently utilized in premises liability litigation.

The assessment of each security risk can be expressed in a number of ways, such as low, medium, or high on a scale of 1 to 10. The higher the risk, the greater the effort

required to implement safeguards that will provide an adequate level of protection. [Figure 3-3](#) is an example of a matrix used to list the security risks and address the degree, or level, of risk for specified areas or functions.

Risk levels should be expressed in terms of addressing the threat by considering the safeguards already in place, and not the prevalence of the risk. For example, the risk of fire is well known; however, a well-trained staff, fire control construction, fire-safe practices, and physical fire detection and control equipment may relate to fire being a very low risk for the organization.

## Example of a Security Risk Assessment Worksheet

### *Matching Safeguards to Risk*

After the risk assessment is completed and the degree of risk calculated, each risk is viewed in relation to the safeguards currently in place and additional safeguards that may be needed to maintain an acceptable risk level. In some cases the safeguards are the direct responsibility of the security function, and in others a specific operating department may be responsible. Seldom is the application of all safeguards the responsibility of one particular department; rather, responsibility is usually a combination of security and the operating department. Often, the management of security risks is the function of the hospital's Environment of Care Committee. Further, a given safeguard applied to a specific risk will, in many cases, also bear on many other vulnerabilities. For example, the security officer is a safeguard utilized to help manage a high percentage of all the known risks.

In assessing risk and applying safeguards the security professional is concerned not only with existing risks, evidenced in part by incidents, but also with potential risk, as prevention is a key concept. In practical terms, it is difficult to obtain resources and gain organizational support for preventive safeguards. Unfortunately many safeguards currently in place are due to past incidents, and were put in place as a reactive measure without sound planning and rational justification.

Security program safeguards should have some relation to the level of threat. [Figure 3-4](#) depicts a concept of an identified threat level to risk categories and the corresponding safeguards. The basic thought is simply that of applying safeguards commensurate with the level of risk to avoid unnecessary cost and operational inconvenience. In terms of cost, the healthcare security administrator will be frequently tasked with addressing the return on investment (ROI) of various components or elements of the current protection system and in terms of requesting new or upgraded security, manpower, or equipment.

In this section of the text the main focus has been on identifying security risks and assessing risk rather than on reviewing the specific safeguards and their applications. The following example, however, will help the reader to understand the conceptual model of matching safeguards and multidepartment responsibilities in managing a specific risk. In this example the stated risk is protecting people in various facility parking lots.

Risk Identified: Personal safety in parking areas

Safeguards Implemented:



## RISK POSTURE SELF-ASSESSMENT DEFINITIONS &amp; VALUES

Measurement	Definition	Risk Value
<b>Physical Setting</b>		
<b>CAMPUS SIZE</b>	Number of acres (include all areas for which the security effort is responsible)	Capture value only
<b>BUILDING SIZE</b>	Total amount of occupied square feet (include all areas for which the security effort is responsible)	Capture value only
<b>PARKING</b>	Number of spaces in parking garages and on surface lots for which the security effort is responsible	Capture value only
<b>FACILITY STAFF SIZE (FTES)</b>	Number of weekly hours worked by contract, paid, and volunteer staff at the organization divided by 40 resulting in the full-time equivalent value	Capture value only
<b># OF SECURITY FTE'S</b>	Number of security officer positions equal to 2,080 hours/year	Capture value only
<b>High-Risk Services Rendered</b>		
<b>INTENSIVE CARE SERVICES</b>	The facility has dedicated intensive care services	Yes =
		No = 0
<b>MOTHER/BABY</b>	The facility has a dedicated mother/baby unit to include labor and delivery and postpartum services	Yes =
		No = 0
<b>NEONATAL INTENSIVE CARE</b>	The facility has a dedicated neonatal intensive care unit (any level)	Yes =
		No = 0
<b>PEDIATRIC INPATIENT/ICU</b>	The facility has a dedicated pediatric patient care unit or pediatric intensive care unit	Yes =
		No = 0
<b>FORENSIC PATIENT RECEIVING UNIT</b>	The facility has a dedicated forensic patient intake center or is a recognized receiving correctional healthcare facility	Yes =
		No = 0
<b>INPATIENT PSYCH UNIT</b>	The facility has a dedicated psychiatric intake center or is a recognized receiving behavioral health center for adult, geriatric, or adolescent patients or chemical dependency	Yes =
		No = 0
<b>General Service Volumes</b>		
<b>ADJ PT DAYS</b>	Adjusted Patient Days	0 = 0 1 – 40,000 = 1 40,001 – 80,000 = 2 80,001 – 120,000 = 3 >120,000 = 4

FIGURE 3-3 An example of a security risk assessment worksheet.

<b>BIRTHS</b>	Number of annualized live births	0 = 0 1 – 100 = 1 101 – 2000 = 2 2001 – 3000 = 3 >3000 = 4
<b>PEDIATRIC PATIENTS</b>	Number of annualized pediatric patient visits	0 = 0 1 – 100 = 1 101 – 2000 = 2 2001 – 3000 = 3 >3000 = 4
<b>FORENSIC PATIENTS</b>	Number of annualized forensic patient visits	0 = 0 1 – 50 = 1 51 – 100 = 2 101 – 499 = 3 >500 = 4
<b>INVOLUNTARY PSYCH HOLDS</b>	Number of annualized involuntary psychiatric patient holds; i.e., Baker Acts, mental health holds, alcohol holds, and 5150s.	0 = 0 1 – 50 = 1 51 – 100 = 2 101 – 499 = 3 >500 = 4
<b>VIP PATIENTS</b>	Number of annualized patients that pose special security problems and require special security precautions; i.e., risk of targeted violence (victim of domestic violence, gang affiliation, and witness to a crime, etc.) dignitary, or other high-profile personality	0 = 0 1 – 3 = 1 4 – 6 = 2 7 – 9 = 3 >10 = 4
<b>Emergency Services</b>		
<b>TRAUMA LEVEL</b>	<p><i>Level 1</i> – A regional resource trauma center, which is capable of providing total care for every aspect of injury and plays a leadership role in trauma research and education</p> <p><i>Level 2</i> – A community trauma center, which is capable of providing trauma care to all but the most severely injured patients who require highly specialized care</p> <p><i>Level 3</i> – A rural trauma hospital, which is capable of providing care to a large number of injury victims and can resuscitate and stabilize more severely injured patients so they can be transported to Level 1 or 2 facilities</p>	<p>Level 1 = 4</p> <p>Level 2 = 3</p> <p>Level 3 and all others = 1</p>
<b>ED VISITS</b>	Number of annualized patient visits	0 = 0 1 – 20,000 = 1 20,001 – 40,000 = 2 40,001 – 60,000 = 3 >60,000 = 4

FIGURE 3-3 (Continued)

<b># PATIENT ASSISTS</b>	Annualized number of security officer interventions involving at-risk patients	0 = 0 1 – 100 = 1 101 – 250 = 2 251 – 400 = 3 >400 = 4
<b>AVERAGE TIME ON PATIENT ASSIST</b>	Average time spent assigned to monitor a patient's activities in order to prevent harm to self, staff, or others	0 = 0 1 min. – 30 min. = 1 31 min. – 60 min. = 2 61 min. – 90 min. = 3 >90 min. = 4
<b>CAP INDEX CRIMECAST MODEL</b>		
<b>CAP INDEX CRIMECAST (National Score)</b>	Probability for crime to occur in context with the national levels of criminality	0 = 0 1 – 100 = 1 101 – 200 = 2 200 – 350 = 3 >350 = 4
<b>Security-Related Responses</b>		
<b>CRIMES AGAINST PROPERTY (FACILITY INCIDENTS)</b>	Number of theft (larceny) and burglary reports of events occurring on facility property, whether founded or unfounded through subsequent investigation	0 = 0 1 – 3 = 1 4 – 6 = 2 7 – 9 = 3 >10 = 4
<b>CRIMES AGAINST PERSONS (FACILITY INCIDENTS OF VIOLENCE)</b>	Number of abduction, assault, car-jacking, murder, non-negligent manslaughter, suicide, rape, robbery, whether founded or unfounded through subsequent investigation	0 = 0 1 or more = 4
<b>AGGRESSIVE WEAPONS ON CAMPUS</b>	Number of handgun, hatchet, knife with blade > 3", long-barreled gun, etc. identified, procured, or found on campus	0 = 0 1 = 1 2 = 2 3 = 3 4 or more = 4
<b>POLICE RESPONSES</b>	Number of requests made for events occurring on facility property requiring law enforcement response	0 = 0 1 – 5 = 1 6 – 10 = 2 11 – 15 = 3 >15 = 4

FIGURE 3-3 (Continued)

### 1. Security Force:

- Patrol parking areas;
- Fixed post assignments during specific shift changes;
- Escort people on request;

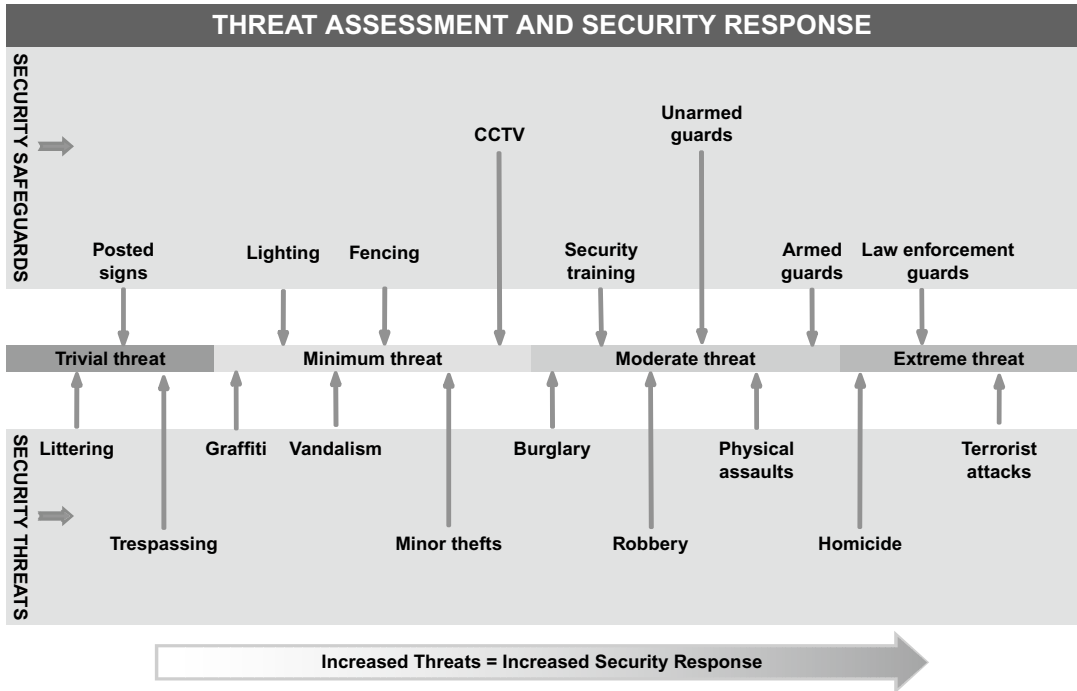


FIGURE 3-4 Security threat assessment and physical security safeguards.

- Provide various departmental in-service education programs;
  - Follow up and investigate incidents.
2. Install emergency communication devices in strategic and highly visible locations that are connected directly to the security dispatch center.
  3. Monitor by closed circuit television (CCTV) designated parking areas.
  4. Operating Departments:
    - Standardize work shifts with other departments when possible;
    - Advise employees of security escort service.
  5. Provide adequate night lighting.
  6. Check trees and shrubs for proper placement and keep well pruned.
  7. Personnel Department:
    - Provide parking lot safety and security services information to new employees;
    - Address parking lot safety and security services in the employee handbook.
  8. Nursing/Admissions:
    - Inform visitors and patients of security escort services and means of requesting this service.

As one can readily see, the above safeguards and defined responsibilities are somewhat similar to those that would be considered in addressing the risk of break-ins and damage to vehicles in the parking areas.

## A Continuous Process

Once the process of risk assessment has been completed, an abatement plan has been devised, and safeguards have been blended into a security program, this process begins again. The identification of security vulnerabilities and risks is ongoing. Risks previously identified may no longer exist, and new risks may appear as the dynamics of a healthcare environment continually changes.

### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #01.02

#### **SECURITY RISK ASSESSMENTS**

**STATEMENT:** Security Risk Assessments will be conducted on a regular and ongoing basis. The objective of the Security Risk Assessment is to identify assets of the healthcare facilities (HCFs) or healthcare organization's (HCOs) primary mission and operations, threats to and vulnerabilities of those assets, and develop reasonable risk mitigation strategies to protect assets.

#### **INTENT:**

- a. Security risk assessment should be conducted by a qualified professional who has training and experience in healthcare security.
- b. Identify assets of the HCF/HCO. People assets may include direct care providers and patients along with other persons such as visitors, family, and support personnel. Property assets include not only buildings but tangible assets used to provide patient care (such as medical gases, medical equipment, utilities, and supply lines), intangible assets such as the organization's reputation, and information assets.
- c. Inventory current security measures in place to protect critical assets including policies and procedures, physical/electronic security equipment and systems, and security personnel. The inventory process should include a review of all available security documentation such as security plans, security officer deployment, training, and post orders. The inventory may be accomplished using an outside-in approach (begin at the perimeter and work toward the identified critical assets through each line of defense) or an inside-out approach (begin at each critical asset and work out to the perimeter).
- d. Assess quantitative and qualitative threats to the organization's assets. This may be accomplished by obtaining and reviewing the area police crime statistics and security reports for at least the prior 3 years to determine types of incidents, problem areas on campus, times and frequency of occurrence. It is also recommended that threats be identified through the exchange of information with similar organizations and public law enforcement agencies, the review of industry publications, and discussions with facility staff.
- e. Consider improvements of the organization's protection of assets in light of the threats to and vulnerabilities identified to determine security enhancements needed to mitigate risks. A cost-benefit analysis of options may be needed to select appropriate measures that reduce risks to an acceptable level and comply with applicable healthcare industry standards, guidelines, and regulatory agency requirements.

- f. Results of formal risk assessments should be documented for ongoing review and forwarded to appropriate leadership.

**REFERENCES/GENERAL INFORMATION:**

- Colling, R. L. (2001). *Hospital and healthcare security* (4th ed.). Woburn: Butterworth-Heinemann.
- Vellani, K. H. (2006). *Strategic security management: A risk assessment guide to decision makers*. Woburn: Butterworth-Heinemann.
- Risk Assessment Toolkit CD, IAHS, October 2008.

**Approved:** April 2009.

## References

1. Silver, J. (2008, July 23). Elderly man beaten by hospital roommate. *Pittsburgh Post-Gazette*. Retrieved from <http://www.post-gazette.com/pg/08205/898759-57.stm>.
2. Huard, R. (2006, September 1). Ex-hospital Nurse Irvin pleads guilty to molesting, trafficking. *Union-Tribune*. Retrieved from <http://www.signonsandiego.com/news/metro/20060901-1220-bn01irvin.html>.
3. Arrest made in hospital rape; suspect recently out of jail. (2005, July 1). *The Post Standard*.
4. Milburn, J. (2008, February 8). Three fatally shot in Girard. *Topeka Capital-Journal*. Retrieved from [http://www.cjonline.com/stories/020800/kan\\_girard.shtml](http://www.cjonline.com/stories/020800/kan_girard.shtml).
5. In brief, bomb threat. (2002). *Hospital Security and Safety Management*, 22(12).
6. Bomb threat causes Canadian hospital to increase security. (2007, November 30). *Campus Safety Magazine*, November/December 2008. Retrieved June 14, 2009 from <http://www.campusafetymagazine.com/News/Default.aspx?NewsID=1583>.
7. Two bomb scares offer this hospital a chance to upgrade its planning. (2007, September). *Briefings on Hospital Safety*, 15(9), 1.
8. Zachariah, H. (2008, November 2). Smoke bomb tossed into Memorial Hospital, *The Columbus Dispatch*. Retrieved from [http://www.dispatch.com/live/content/local\\_news/stories/2008/11/02/hosp03.html](http://www.dispatch.com/live/content/local_news/stories/2008/11/02/hosp03.html).
9. Phony technician makes costly repair (2004, November). *Healthcare Security and Emergency Management*, 13(11), 12.
10. Thieves steal copper from hospital restrooms. (2007, December 10). *Healthcare Security Weekly*. Retrieved June 14, 2009, from <http://www.hcpro.com/HOM-201801-1423/Thieves-steal-copper-from-hospital-restrooms.html>.
11. Pankratz, H. (2008, November 20). Nurse arrested in drug thefts. *Denver Post*. Retrieved from [http://www.denverpost.com/search/ci\\_11026752](http://www.denverpost.com/search/ci_11026752).
12. Two major hospitals implement random drug testing for anesthesiologists. (2008, November 13). *Campus Safety Magazine*. Retrieved June 14, 2009, from <http://www.campusafetymagazine.com/News/?NewsID=2346>.
13. Standoff in IL turns deadly. (2007, January). *Briefings on Hospital Safety*, 8.

14. Grudge turns deadly at hospital. (2008, March 29). *Rocky Mountain News*, 23.
15. Smith, T. A. (2007/2008). Patient prisoner security—a call to action. Retrieved March 28, 2009, from <http://www.ihf-fih.org/pdf/59-61%20%20Smith.pdf>.
16. 7 residents, 1 nurse die in N.C. nursing home shooting. (2009, March 29). *Charlotte Observer*. Retrieved March 30, 2009, from <http://www.charlotteobserver.com/597/story/630317.html>.
17. Ex-nurse says he killed patients. (2003, December 16). *Denver Post*, 2A.
18. Gangland-style slaying of patient by 5 masked gunmen stuns islands. (2008, May 22). *The Virgin Islands Daily News*, 1–3.
19. Virginia Fusion Center. (2005, March 18). *Intelligence bulletin #05-11*. Virginia: Department of Virginia State Police.
20. Hospital intruders puzzle officials, raise concerns about safety. (2005, March 3). *ASIS Security Management Daily*, 3.
21. Man turns the tables on hospital police and security. (2008, April 4). *CBS News*. Retrieved from <http://cbs4.com/local/Deranged.Man.Crazy.2.692301.html>.
22. Ask the auditor: Guarding against employee fraud and theft in healthcare organizations. (2007, May 15). *ASIS Security Management Daily*, 3.
23. UPMC has new procedure to find missing patients. (2009, January 3). *Pittsburgh Post-Gazette*.
24. Rowley, J. (1997, November 14). Survey: 1 in 12 women stalked at least once. *Rocky Mountain News*, 44A.
25. Wade E. (1999, January 18). Medical equipment theft memo. *Florida Hospital Association*, 1.
26. Clark, J. P., & Hollinger, R. C. (1980). Theft by employees. *Security Management* (September).
27. Kennedy, D. B. (1989). Case your space. *Security Management*, 47(April).

# Security Management Planning

Security management planning involves the formulation of two basic interrelated but separate types of plans. The first is a *security management plan* that relates directly to the day-to-day protection program of the organization. This plan should be considered as a short-term plan which requires a formal review, evaluation, and modification on an annual basis. It is also a living document that can, and should, change as circumstances and situations develop. The second plan is the *security strategic plan* which relates more toward community involvement, long-term goals, objectives, philosophy, and program direction. The strategic plan can be defined as a “road map” (or master plan) enabling the organization to move forward toward its destination (goals) in an orderly, defined, and efficient pathway.

## Security Management Plan

A Security Management Plan (SMP) is a description of the protection program developed for an organization after evaluating security risks and threats to the organization. There are various “schools of thought” on how general or all inclusive such a plan should be. An SMP, however, is a necessary element of managing any healthcare organization. IAHS has developed a guideline which outlines the basic aspects of such a plan.

There is no set format for a plan for security management and the plan can vary in length from a few pages to many. The plan should be just that—a plan—and should not generally include policy and procedure in any great detail. It is an operational plan and should address all major components of the security program. In a sense, it equates to a brief business plan without the financial aspects of a typical business plan.

In addition to the intents of the IAHS guideline other areas that may be included in the SMP are:

- A listing of physical security safeguards as elements of the program;
- A listing of the department operating policies and procedures including preparation and review protocols;



**IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #01.01****Security Management Plan**

**STATEMENT:** Healthcare facilities (HCFs) must develop an SMP. The plan should include preventive, protective, and response measures designed to provide a safe environment.

**INTENT:**

- a. The plan should be based on the security risk assessment and needs of the HCF.
- b. The plan should include, but not be limited to:
  1. Security program mission statement;
  2. Statement of program authority (e.g., a facility organization chart depicting reporting levels);
  3. Identification of security sensitive areas;
  4. An overview of security program duties and activities;
  5. Documentation system (i.e., records and reports);
  6. Training of security staff and “general facility staff”;
  7. Planned liaison activity with local public safety agencies;
  8. Security personnel summary, position descriptions;
  9. A copy of the most recent SMP evaluation report.
- c. The plan should be evaluated annually, as well as modified as required as an ongoing activity. Annual reviews should be evidenced by affixing the evaluation date to the plan.

**REFERENCES/GENERAL INFORMATION:**

- Security Issues for Today’s Health Care Organization, Joint Commission on Accreditation of Healthcare Organizations, Oakbrook Terrace, IL, 2002.

**Approved:** January 2006

**Last Revised:** October 2008

- Organization staff and others as applicable (i.e., patients, vendors, visitors, neighborhood);
- Program performance standards;
- Measurement and improvement strategies.

## Security Mission Statement

The security mission statement is the foundation of the security program and essentially states the reason or purpose of the program—its goal of providing a reasonably safe and secure environment for patients, visitors, employees, volunteers, medical staff, and vendors. The security mission must relate to, and support, the overall mission, vision, and core values of the organization. [Figure 4-1](#) provides an example of a healthcare security

---

**UNITED GENERAL HOSPITAL**  
**SECURITY MISSION STATEMENT**

The mission of security at United General Hospital (UGH) is to provide a reasonable and prudent level of protection from harm to all persons utilizing the campus of UGH and the protection of property. Security will also be responsible to provide a myriad of general services that will facilitate the efficient delivery of services and courtesies to visitors, staff, and patients.

The security department will be responsible to identify security risks, design protection safeguards to properly manage these risks, implement and manage security safeguards, evaluate effectiveness of safeguards, and improve systems of protection within a framework of cost effectiveness, efficiency, and consistent with the overall mission of the organization.

The security department will provide direct protection services, while assisting, educating, and coordinating the security efforts of all staff members and departments.

The security department will be responsible to coordinate the UGH protection effort with public safety agencies, regulatory agencies, and healthcare organization where the issues of security or law enforcement is involved. The specific goals, objectives, systems, and procedures of security operations will be delineated in the UGH Security Management Plan.

---

**FIGURE 4-1** Security mission statement.

mission statement. Embedded within the mission statement should be the scope of locations covered by the plan.

### Program Authority

The authority and responsibility for the day-to-day operation of a security program must be assigned to a specific position within the organization. The day-to-day tasks of security may be delegated to others; however, the responsibility for getting the job done rests with the specific position designated by organization leadership. In most cases this position will be displayed in an organization chart. In some cases an organization chart may only portray the function rather than a specific position. In this case the SMP should contain a written directive from the chief executive officer or the chief operating officer delegating authority to a specific position to manage the security program. In larger organizations this authority would generally be conferred upon the Director or Manager of Security. In small organizations it may be the Director of Facilities, Director of Human Resources, or another high-level administrative position. IAHS guideline #02.01 outlines the basic aspects of authority and responsibility of this leadership position.

**IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.01****Security Administrator**

**STATEMENT:** Security Administrators play a critical leadership role in an HCF's security management program.

**INTENT:**

- a. Each HCF should identify a person, designated by leadership, to be charged with primary responsibility for the security function.
- b. Security Administrators should possess policy-making authority in keeping with the review and approval process of the HCF.
- c. Security Administrators should possess the authority to immediately and independently address any imminent threat that may result in serious bodily injury, death, or in significant loss of property. This authority should include standing authorization to deploy and implement interim security measures.
- d. Security Administrators should be involved at the onset of design through completion in the planning and building phases of all new facility construction and renovations.
- e. Provision should be made to allow the Security Administrator to maintain a current level of understanding of emerging threat identification techniques and responses. Membership in at least one professional security organization and participation in security educational programs is strongly encouraged.

**REFERENCES/GENERAL INFORMATION:**

- International Association for Healthcare Security & Safety, P.O. Box 5038, Glendale Heights IL, 60139.
- ASIS International, 1625 Prince Street, Alexandria VA, 22314.

**Approved:** January 2006

**Last Revised:** October 2008

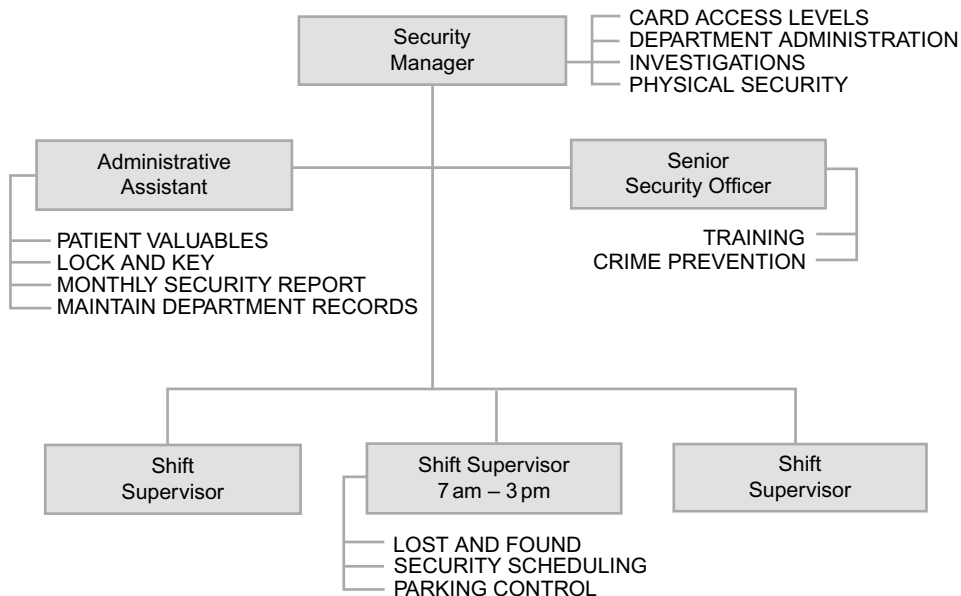
An important component across the delivery of healthcare regardless of country or government involvement, the National Health Service (NHS) in the United Kingdom, requires each Health Trust to have a Security Management Director, a member of the Executive, designated with administrative responsibility for security. Each Trust is also required to identify a Local Security Management Specialist (LSMS) who has responsibility for the day-to-day operation of the protection program and is trained and credentialed by the Security Management Service of the NHS. The LSMS can be a stand-alone security administrator or someone who has multiple functional responsibilities; that is, Health and Safety or Facilities. In Canada, the requirement is not as prescriptive, and Accreditation Canada, unlike like TJC, is largely silent on the designation of a leadership position to be charged with oversight of the security function. The Canadian regulations are relatively clear, in most provinces, in requiring a designated lead in health organizations

to lead a program for the prevention and management of aggressive behavior against staff—largely through workplace safety legislation. However, the requirement for overall security leadership is not in place.

When the organization chart is included in the SMP, it must portray at least the next highest hierarchical position, or reporting level, above that of the security administrator position. In most cases the organization chart will show reporting levels at least to the chief operating officer level. An organization chart may also show how the security department or program is organized. The department organization chart may be organized to show program functions, positions, or a combination of both position and function. A program organization chart can be quite helpful in conveying an understanding of the overall picture or concept of the security program. [Figure 4-2](#) is an example of a security program organization chart showing a combination of positions as well as functions.

### Risk Assessment Evaluation

In this section of the SMP it is important that the methodology and conclusions of the organization security risk assessment be addressed. It is recognized that organizational security risk assessment is a living, day-to-day, continuous process. In this respect each year there should be a formal review of the risk status of the various threats but not necessarily as in depth as the baseline (initial) assessment, which may be many years old. The conclusions of this annual security risk assessment review and goals for the new year may actually be included in the annual review of the SMP. It is common practice to use the calendar year



**FIGURE 4-2** Security program organization chart depicting positions and functions.

(i.e., January–December) for the purpose of review and goal setting. This practice renders the reporting periods to be compared in a clear and consistent manner.

## Identification of Security Sensitive Areas

Each healthcare organization must identify those areas that they consider the most security sensitive. This evaluation would be part of the objective of the overall risk assessment process. There is no real clear definition (criteria) of what is, or is not, a security sensitive area for a specific organization. Security sensitive areas should not be necessarily confused with areas of high concern. As an example, safety and security of persons utilizing a parking structure may be of high concern, but would not normally be considered a security sensitive area. The rationale would be that security breaches in the parking area would not severely impact the mission of the organization, as would security breaches in the emergency department relative to the safe and secure delivery of patient care. *Chapter 20, Security Sensitive Areas*, covers this subject in much greater detail.

## Security Staff Position Descriptions

The SMP should contain a brief description of the activities performed by each job position of the security department. An option for this section of the plan could be to include the complete position descriptions in an appendix or attachment to the plan and simply refer the reader to that document. In utilizing this option it may be useful to include an appendix for other areas of the plan such as defining skill and competency levels of various positions, a listing of general activities/duties, and a listing or table of contents of security policies and procedures.

This section of the plan is also a good place to include the number of authorized full-time equivalent (FTE) staff for each position. In place of the number of staff for each position, an alternative could be the number of weekly hours required to staff and operate the program. [Table 4-1](#) is an example of portraying staff requirements as an FTE count and the number of deployment hours.

**Table 4-1** Security Department Authorized Staffing Level

Position	FTE	Hours/Week
Security Manager*	1.0	40
Investigator/Trainer*	1.0	40
Shift Supervisor	4.0	160
Security Officer I	11.4	456
Security Officer II	10.6	424
Totals	26.0	1040

\*Salaried positions.

## Security Program Overview (Duties and Activities)

This section of the SMP is intended to provide the reader an understanding of what the program does (operations) on a day-to-day basis. This overview bridges the gap between mission statement, organization charts, and position descriptions as to the activities performed or accomplished by the security program.

## Security Physical Safeguards

All security programs utilize physical security safeguards to some degree. In this section of the plan each safeguard should be listed with a general description and how the security program utilizes the safeguard to include safeguard objectives, responsibility for systems operation, and maintenance. [Figure 4-3](#) is an example of how a physical safeguard might appear in the SMP.

### PHYSICAL SECURITY

---

#### SYSTEM DESCRIPTION/PROTOCOL

TYPE: Closed Circuit Television (CCTV)  
 LOCATION: 4 North Newborn Nursery and Post Partum (Mother/Infant)  
 OBJECTIVE: General Surveillance/Recorded Movement

GENERAL DESCRIPTION: This CCTV system utilizes four color cameras, a quad (4 screen) monitor, and a recording system. The recording system tapes images from all four cameras, and a ten-day library of recorded images is maintained. The system monitor is located at the 4 North nursing station. It is intended that there will be live monitoring of the cameras only when staff randomly look at monitors or when there is a specific situation requiring attention.

CAMERA LOCATION/PURPOSE: Camera #1 is mounted in the ceiling of the main corridor entry to the mother/infant unit. The purpose of the camera is to record all persons entering the unit.

Camera #2 is mounted in the ceiling of the main corridor entry to the unit back-to-back of Camera #1. The purpose of this camera is to record all persons exiting the unit via this unit corridor.

Camera #3 is mounted in the ceiling of the unit's back corridor (W-E). This corridor cannot be visualized from the nursing station. There is a door at the end of this corridor, leading to a main facility corridor. This door is locked from the main corridor side. The camera is positioned to record all exiting persons and to provide staff at the nursing station a view of this unit's corridor when desired.

Camera #4 is mounted in stairwell #8 facing the stairwell exit door of the mother/infant unit. The purpose of this camera is to view any person exiting into the stairwell. The door is equipped with a 15-second delayed exit device and locked from the ingress side. An alarm is sounded at the nursing station immediately when pressure is exerted on the exit release bar on the door. Staff will immediately respond to the exit door when the alarm is activated.

**FIGURE 4-3** An SMP description of an organization's utilization of CCTV.

## Security Staff Training

In this section of the plan there will be a review of the various elements of the training provided to security personnel. This training will vary considerably between organizations but will always relate directly to the job description and skill levels required of each position. Since skill levels, training, and competency all tie together, this section would be a good place to include competency procedures. Competency essentially means verifying skill levels and/or determining the training needs of each staff person to achieve the desired level of identified skills necessary to satisfactorily perform in the assigned position.

## Department Policies and Procedures

A simple listing of security operational policies and procedures is appropriate for this section. This information is often referred to as post orders, general orders, facility orders, security policy, and procedures. A brief explanation of the process of how these policies and procedures are prepared, approvals required, and how and where they are maintained in a current status would help the reader in understanding the mechanics of this element of the security system. The policy and procedure listing referred to in this section does not include personnel policies covering staff conduct, disciplinary actions, pay, or benefits. [Figure 4-4](#) is an example of commonly utilized security policy and procedures.

## Security Education (Security Awareness)

A comprehensive security program will include a program of education, training, and motivating persons to be security aware. Being security aware and adhering to good security practices prevents security incidents. While much of this educational effort is directed to staff, it should be clear in this section of the plan that is responsible to provide the various education activities. For example, the security department may be responsible for new employee security training or it may be the human resources department. Another example is the requirement for staff training relative to security in designated security sensitive areas. Is this training the responsibility of the area supervisor or is it accomplished by the security department? Who develops training material? Where and how are the training records maintained?

The typical security program will involve a variety of departments to accomplish employee security training. The security department should provide the coordination, education, and consultation to blend all these efforts into the overall unified security training program. Frequently shared information that many medical centers provide their employees include security-related information such as:

- Identification badges;
- Security services phone number;
- Reportable incidents (disturbances, patient, visitor, employee lost/stolen property, suspicious people/items, smoking on campus);

## COMMON HEALTHCARE SECURITY POLICIES AND PROCEDURES

- Security Staffing and Deployment
- Functional Relationship of Security Department Positions
- General Security Officer Duties and Activities
- Utilization of Security Equipment and Vehicles
- Reporting for Duty
- Security Assistance/Support
  - Patients
  - Staff
  - Visitors
  - Vehicle
  - Departments/Programs
- Critical Incident and Alarm Response
- Outside Agency Interaction/Response
- Legal Actions and Guidelines
- Investigative Procedures
- Report Preparation
- Facility Access Control
- Enforcing Organization Rules
- Safety Services/Response
- Parking Control
- Facility Property Control/Removal
- Patient Property Control
- Lost and Found
- Security Officer Training
  - Helicopter Landings
  - Bomb Threats
  - No Smoking Enforcement
  - Forensic Patients
  - Searching for Contraband
  - Emergency Management Response
  - Use of Force

**FIGURE 4-4** A list of common healthcare security policies and procedures.



- Weapons;
- Prisoner (forensic) patients;
- Access control (keys, cards, codes, business hours versus after-hours, parking, visitor management, assistance alarms);
- Securing personal items;
- Infant abduction prevention and response;
- Department-specific security information.

*Chapter 15, Employee Involvement and Security Awareness*, covers the subject of employee involvement/security awareness in the healthcare protection program in greater detail.

### Public Safety Agency Liaison

In this section of the SMP, only a brief discussion of the relationship and coordination with the various public safety agencies is required. Information included would identify the law enforcement organizations that have jurisdiction and the emergency service agencies that are responsible to provide emergency services to the facility. Operational and protocol procedures with these agencies would generally not be referred to in the SMP.

### Security Records and Reports

The SMP should outline basic security records and reports prepared and utilized in the security program. In this outline there should be a brief explanation of the objective of each document, who is responsible for preparation of the document, distribution protocols, how and where each document is available for review, guidelines for follow-up/improvement activities, and the assigned document retention time period. [Figure 4-5](#) is a sample format that would be prepared for each document (form) that is utilized in the security program.

### Performance Standards and Performance Improvement Measures

There must be program performance standards to determine if program goals and objectives are to be accomplished. A program must measure actual activity to determine the level of service provided. A goal of all programs would be to develop a plan of improvement action for activities not meeting standards and in addition look for opportunities to set higher standards where possible. When an adverse change occurs, the leaders assess the relative severity of the change and determine an appropriate response. [Table 4-2](#) identifies sample performance measures for event elements within the protection program. Many organizations will also monitor program and activity elements to address preventive and compliance activities.

A key management responsibility is to ensure that standards are set at a realistic level. If standards are too low the program stagnates with little incentive to improve. On

## SECURITY DOCUMENTATION

---

### SYSTEM DESCRIPTION/PROTOCOL

TYPE: Security Incident Report

LOCATION: All Campus Facilities

OBJECTIVE: The completion of an accurate and timely report of all security incidents occurring on facility property, or affecting the organization from a protection perspective. The report will clearly set forth facts and include all actions taken by personnel in relation to the incident.

#### GENERAL DESCRIPTION

Security Incident Reports (SIR), form SD-104, will be completed by the assigned security officer responding to the incident or by off-site personnel as directed by a member of the security department. The SIR will be completed as soon after the initial management of the incident has been accomplished. The completed report will be reviewed by the security shift supervisor and be placed in the investigator's "in box" located in the central security control station.

#### REPORT UTILIZATION

The security shift supervisor, or the assigned investigator, will effect any emergency or routine notification of other appropriate parties relative to a security incident.

The assigned investigator will determine the need for any follow-up investigation of the incident and if so will coordinate this follow-up activity. The investigator will enter summary incident information into the computer log file after verifying the appropriate incident report classification. The computer log file will be utilized to generate the monthly, quarterly, and annual security incident report utilized by security administration and reporting to the facility safety committee.

#### REPORT STORAGE/RETENTION

The completed SIR, with attached supplemental reports if appropriate, will be filed chronologically as the master file. These reports will be maintained for a 5-year period except for a report where there is a perceived need for the report to be maintained in excess of 5 years. Retention of these reports will be determined on an individual basis by the Director of Security.

**FIGURE 4-5** A sample format for explaining the security incident report in the SMP.

the other hand, standards must be realistically achievable. IAHS guideline #06.01 outlines the basic aspects of standards and improving performance.

### TJC Standards (2009)

The SMP should address how each TJC accredited, or nonaccredited, US healthcare organization complies with each specific Element of Performance (EP) of the standards pertaining to security. The plan should not, however, be limited to just the TJC requirements. Simply addressing the TJC standards and elements alone will not provide a complete and comprehensive protection plan for the organization.

**Table 4-2** Sample Security Department Performance Measurements

Performance Measures—Security Event Elements				
Measure Description	Period	Trigger Value	Actual Value	Action(s) Taken When Actual Value Exceeds Trigger Value
The average number of Patient Assistance-ER events, in a quarter, does not exceed the 2009 average	Q1 = 121	+5%	211	
	Q2 = 202		255	
	Q3 = 198		249	
	Q4 = 255		303	
The average amount of time spent on Patient Assistance-ER events, in a quarter, does not exceed by 5% the 2009 average	Q1 = 2:15	+5%	3:02	
	Q2 = 2:49		3:45	
	Q3 = 3:18		4:13	
	Q4 = 3:02		2:58	
The average number of “crime-related” events (assault, burglary, missing property, stolen or whole vehicle, murder, robbery, suicide, vandalism), in a quarter, do not exceed 2009 average	Q1 = 4	Anything > avg.	2	
	Q2 = 0		2	
	Q3 = 1		0	
	Q4 = 5		3	
The average number of “open door/window” conditions, in a quarter, do not exceed the 2007 average	Q1 = 77	+5%	64	
	Q2 = 44		45	
	Q3 = 31		25	
	Q4 = 54		60	

**IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #06.01****Program Measurement/Improvement—General**

**STATEMENT:** Healthcare facilities (HCF) will formally evaluate the effectiveness of their security system on a regularly scheduled basis and will identify areas in which program improvement is appropriate. Goals, process for improvement, and elements for measuring progress will be identified in the Security Management Plan or in a security improvement performance plan.

**INTENT:**

- a. It is essential that a system of performance measurement(s) be in place to evaluate the level of security services being provided.
- b. The improvement of security performance and achievement of improvement goals is an ongoing and continuous process.
- c. Performance measures are required to evaluate the effectiveness and management of the program. Performance measurement should be goal-driven. If a goal is to reduce a certain activity or increase a perception of security, the measurement should reflect a starting and an ending point.

- d. The tools to gain information should be reliable and consistently used from one measuring time to the next. Charts, graphs, and other visual enhancements may be useful in presenting the data in a concise and clear manner.
- e. Trending of performance data is a common methodology of benchmarking selected elements of security performance or in analyzing elements of program activity and incidents. A basic security, and essential, element of a security program is to track security incidents. A statistical summary of past security incidents, by incident category, should be maintained on a monthly basis. This summary should portray the number of incidents on a month-to-month report. This report would compare the current month and previous months to allow a trend analysis for at least a 12-month period and year-to-year.

**Approved:** October 2008

There were two major changes affecting security in the 2009 TJC Standards. The first was the combining of Security and Safety into a single standard. The second change was to remove the Emergency Management (EM) Standard from the Environment of Care (EC) Chapter. The EM standard thus became a new stand-alone chapter.

The Safety and Security Standard EC.02.01.01 contains the following EP specific to security:

- The hospital identifies safety and security risks associated with the environment of care. Risks are identified from internal sources such as ongoing monitoring of the environment, results of root cause analysis, results of annual proactive risk assessment of high-risk processes, and from credible external sources such as Sentinel Event Alerts.
- The hospital takes action to minimize or eliminate identified safety and security risks in the physical environment.
- The hospital identifies individuals entering its facilities. Note: The hospital determines which of those individuals requires identification and how to do so.
- The hospital controls access to and from areas it identifies as security sensitive.
- The hospital has written procedures to follow in the event of a security incident, including an infant or pediatric abduction.
- When a security incident occurs, the hospital follows its identified procedures.<sup>1</sup>

Another important safety and security standard, EC 04.01.010, contains the following:

- The hospital established a process(es) for continually monitoring, internally reporting, and investigating security incidents involving patients, staff, or others within its facilities.
- Every 12 months, the hospital evaluates each environment of care management plan, including a review of the plan's objectives, scope, performance, and effectiveness.<sup>2</sup>

The specific components required as part of the annual TJC security plan review should address the following elements:

**Objective:** Review the goal of the SMP and the overall mission of the security department. Do these facilitate a healing environment? Do they help the facility meet its stated mission, vision, and core values? If the objective (or mission) of the department changes, identify the new statement in the evaluation. If the objective of the plan does not change, state that the current objective and mission will continue for the next plan year.

**Scope:** Review the scope of the plan to include verifying all locations covered by the SMP including all off-site locations, new constructions, or acquisitions during the past year. Specifically review each declared security sensitive area and determine if the department will continue to be so declared in the upcoming plan year and identify by name the departments added or subtracted from this declaration and the reason why.

**Performance:** In this section, recap the performance measures/indicators or performance improvement initiatives undertaken for security. Provide the results of each performance standard with an appropriate year-end analysis that includes a specific comment on how effective the measure was to improving the overall security posture at the facility.

Provide year-end statistics for the security incident activity tracked for the past year and if possible, provide a 3–5-year comparison of the data. Denote significant increases/decreases that have occurred, identifying the reasons and any action taken as a response. This same process can be used for the reporting of facility security condition reports.

**Program Effectiveness:** Denote if the plan was effective in meeting its objectives of minimizing physical hazards and managing staff activities to reduce the risk of injury or loss/damage of property. Use this opportunity to discuss the accomplishments of the security department during the past year to include:

- Changes made to the SMP and reasons why;
- Installation/upgrade of physical security measures or electronic security technology to include CCTV cameras or recording devices, duress or intrusion alarms, emergency communication devices or radio systems, access control devices, or lock and key systems;
- Newly written/revised security-specific policy and procedures or security-specific drills conducted to include infant abduction, bomb threat, forensic patient, hostage, VIP, or other;
- Security-specific education and training programs offered to the hospital staff to include the security section of new employee orientation, aggression management/de-escalation, security fairs, personal safety, or other departmental or staff presentations offered;
- Changes (increases/decreases) made to the security-staffing plan or alterations to the deployment/responsibilities of security staff to include assuming responsibility for fire-alarm testing, well-being checks, morgue transports, patient valuables, lost and found, etc.

There are countless accomplishments made by security each year; use this section to comprehensively denote each and use this opportunity to express the value and benefit of security to the facility served.

**Recommendation for Plan Improvement:** Most departments denote a level of success for the security program during the course of the annual review and although TJC does not explicitly require it, a good practice is to denote that opportunities for program improvement exist and stating the goals for the department. Not to be misconstrued with performance indicators or performance improvement initiatives, these goals should identify the strategic initiatives set forth to improve the overall security posture for the upcoming plan year. These recommendations also create an excellent benchmark for determining program effectiveness at the end of the next plan year.

The TJC EM chapter contains a variety of elements that have a direct impact on security operations during an emergency. Standard EM.02.02.05, EP, requires an Operations Plan that describes the following security involvement:

- The hospital's arrangements for internal security and safety.
- How the hospital will coordinate security activities with community security agencies (e.g., police, sheriff, and national guard).
- How the hospital will control entrance into and out of the healthcare facility during an emergency.
- How the hospital will control the movement of individuals within the healthcare facility during an emergency.
- The hospital's arrangements for controlling vehicles that access the healthcare facility during an emergency.<sup>3</sup>

There are, of course, many other aspects of the Emergency Management Plan that will require input, coordination, and support from the security program.

The TJC Human Resources (HR) chapter contains a number of standards that bear directly on the administrative and operational aspects of the security program. Included are the responsibility to establish and verify staff qualifications, orientation of staff, and the implementation of effective staff training. While TJC generally tasks human resources to provide for on-the-job assessment of staff competence and performance, the actual methodology and effort in this regard are the responsibilities of the security program administrator (i.e., the Security Department).

Of particular note for the Security Administrator is the TJC Standard HR.01.04.01 Element of Performance Number 7, which states, "The hospital orients external law enforcement and security personnel on the following:

- How to interact with patients
- Procedures for responding to unusual clinical events and incidents
- The hospital's channels of clinical, security, and administrative communication
- Distinctions between administrative and clinical seclusion and restraint."<sup>4</sup>

An additional information source relative to forensic staff includes the IAHS Basic Security Guideline, “Forensic Patient Security” (02.03), which is further discussed in *Chapter 12, Patient Care Involvement*.

TJC Standards and Elements of Performance should always be reviewed on a periodic basis to determine any additions, deletions, or changes relative to the accreditation process and specific EP requirements.

## Security Management Cycle

There really is no ending point in security management planning and operations. The protection program must be viewed as a cyclical process. It is a dynamic process geared to react to new issues and concerns as well as eliminating ineffective or obsolete practices as an ongoing process. The starting point is, of course, identifying and quantifying security risks as identified in *Chapter 3, Security Risks and Vulnerabilities*. The starting point is repeated day in and day out as the management cycle continues to provide new information. [Figure 4-6](#) reveals the security management process/cycle.

## Security Strategic Plan

The security strategic plan is the second major plan required of the healthcare organization. As opposed to the day-to-day SMP previously discussed, this plan sets the philosophy and direction of the protection program for a longer term (3–5 years) and should include elements of financial planning. The major components of this plan are organization-wide security coordination and control, neighborhood stability and security/crime prevention involvement, public safety agency coordination, criminal justice system interface, a philosophy regarding the type and extent of physical security safeguards to be utilized, the degree of employee/staff involvement in the protection program (i.e., centralization versus decentralization), and building configuration and design

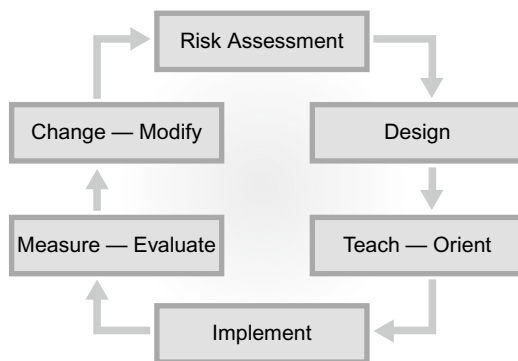


FIGURE 4-6 Security management process/cycle.

considerations. [Figure 4-7](#) illustrates the components of the healthcare organization security strategic plan.

There are various methodologies, approaches, and processes to strategic planning; however, they typically involve the following three-step process to some degree:

- Situation—evaluate the current situation and how it came about.
- Target—define goals and/or objectives that are sometimes referred to as the ideal state.
- Path—map a route to obtain the agreed upon goals and/or objectives.

A major intent of the security strategic plan is to provide the mechanisms and philosophy of achieving the overall direction of the protection system agreed upon by the stakeholders. It should be reflective of guiding beliefs and aligned with daily practices in the protection program. The strategic plan should be sensitive to the overall demographics of the healthcare organization, and explore opportunities for building synergies with other departments and outside agencies.

### Organization-Wide Security Coordination

There must be basic organizational policy that creates a clear understanding of the authority and responsibility of the various layers of management in regard to the protection program. In this respect the security department is seldom responsible for all the components of the protection program either partially or totally. What security responsibility and/or security decisions can be made within an operating department versus those reserved totally for the security department must be clearly articulated. This question



**FIGURE 4-7** Components of the healthcare organization security strategic plan.



involves the philosophy of security centralization versus decentralization. The same questions attach to a multilocation organization that may have two or three campuses and a dozen or more freestanding patient facilities many miles removed from each other. Does security provide all the direct services as a mandate to the freestanding facility or does management at the facility make independent decisions regarding reporting of incidents, key control, alarm systems, etc.? In a totally decentralized approach, the Director of Security on the main campus may serve only as a consultant upon the request of the autonomously operating freestanding facility.

Even within the main facility various departments may be performing security-related functions almost totally removed from the security department. Background checks, including criminal histories, are a significant element of the protection program but may be almost exclusively the responsibility of the human resources department—not only in performing the activity but also in making the decision relative to the depth and methodology of such background investigations.

A small example of the types of questions that must be answered with the preparation of corresponding protocols is:

- Who has the authority, and under what circumstances can the police be called to affect an arrest on behalf of the organization?
- Who has the authority to make decisions in reference to locks and keys? Can any employee order a lock installed, removed, or changed? Who approves the issuance of keys? Who assigns security access levels in a card or biometric access security system?
- Can departments order and install a security alarm or camera in their department without security approval?
- What about physical security safeguard funding? What types of security equipment and supplies are purchased with security department allocated funds versus operating department funds?
- Does the nurse decide if missing property will be reported? If reported does the unit nurse or security representative prepare the missing property report? If the nurse completes the report, is it mandated that a copy be sent to security, nursing administration, or risk management?
- Who decides restitution questions regarding property loss or damage relative to patients, staff, and visitor property?
- When security is called to a patient treatment area due to the inappropriate behavior of a patient or visitor, who is in charge relative to the required actions to be taken?

These questions and many more require clear direction and are instrumental in shaping the type of security program that evolves for the protection of the healthcare organization.

### **Neighborhood Stability and Security/Crime Prevention Activities**

A healthcare security protection program goes beyond the physical property lines of the campus. Community involvement should take place, to some extent, in all protection

programs. The environment surrounding the campus severely impacts the security risks to the organization and all persons coming to and from the facilities. Visitors and staff being assaulted on or off the property may mean little, except in litigation, in terms of creating and maintaining an area where people feel safe. In many cases an incident occurring a block or more from a facility will be reported as being “at the medical center.” Some security departments work at community involvement and others tend to withdraw from this activity. Examples of security community outreach are:

- Security patrols of the neighborhood by organization security departments. These patrols may be funded totally by the healthcare organization, contracted by businesses, or neighborhood associations, or a cost sharing arrangement.
- Active involvement in neighborhood watch and community associations. The healthcare organization may provide funding, meeting places, and sometimes allow use of equipment and attend appropriate community meetings.
- Home purchase assistance is a program to entice staff to relocate to the medical center neighborhood. It is an established fact that owner-occupied living units create an environment that tends to foster improved communities with lower crime rates. These programs all basically operate in the same manner, which provides outright cash and/or low-cost loans to purchase a home. In these programs the employee must agree to personally live in the home for a certain number of years. In addition to organization financial support, there may be legislation that provides tax credits or discount mortgage rates for renovation of living units in historic neighborhoods. Medical centers located in these neighborhoods may find a new source of funds to make owning in the area more attractive.
- Block parties are a popular event, blending the medical area campus into the surrounding neighborhood. These events provide tours, food, entertainment, and fun activities for old and young alike. The concept is to be a good corporate neighbor and an integral part of the community.
- Alarm monitoring and response is another element of community involvement. Alarms generally pertain to businesses; however, a really involved healthcare organization outreach program could provide this service for private homes in their neighborhood as well.

## Public Safety Coordination

The primary public safety agencies that the security program must work with would be homeland security, law enforcement agencies, fire, disaster preparedness and response, and possibly a governmental city-wide ambulance service. The law enforcement coordination presents many additional issues and opportunities. This topic is generally covered in a separate section of the healthcare security strategic plan. In these cases the security strategic plan should include a reference to these important agencies which refer the reader to appropriate documents or departments.

## Criminal Justice Interface

This section of the plan requires specific policy to define appropriate staff interactions with law enforcement agencies at all levels: prosecutors, probation, parole, and correctional personnel. A major issue is what will be reported to law enforcement and who will make these decisions as situations occur. On the surface this appears to be quite simplistic, but as the subsets to these questions develop it becomes more complex. There are confidentiality issues as well as philosophical issues especially between security and the human resources department, which often views the relationship of the organization to staff from different perspectives. The police, on one hand, insist that all crime be immediately reported to them and then politely or otherwise, expound on their overload of work and do not want to be bothered with minor crime. In some jurisdictions the police will not even respond to the scene of certain crimes unless there is a suspect being detained. In this respect, does the organization report the loss of one dollar from the bedside of a patient, 5 dollars, 20, 50, or 100? Or does the organization leave all reporting of missing personal property to the victim? Does the police agency permit, or foster, reporting certain crimes directly to a specialized investigative unit, or must all reporting be accomplished through a police dispatcher or mail-in report? An example is missing narcotics. In many jurisdictions it is appropriate to report directly to the police narcotics unit and in others this direct reporting is prohibited. It is often difficult to define some of these relationships, as law enforcement agencies often give out conflicting information and there is a frequent change in philosophies. These problems have been minimized in some jurisdictions where a specific municipal or county police liaison person has been specifically assigned to work with the healthcare organization (i.e., community policing). There tend to be fewer liaison problems at state and federal levels as contacts are less frequent and issues are more situational with specific decision makers readily available.

## Utilization of Physical Security Safeguards

Virtually all healthcare organizations utilize physical security (hardware) as a component of their protection system. This utilization may include locks, lighting, barriers, and state-of-the-art electronics. Unfortunately, many of our nation's healthcare organizations have ended up with a high-cost, uncoordinated, "conglomeration" of ineffective equipment. Security staffing and physical security safeguards are intended to complement each other in forming a balanced blend of staffing resources and equipment.

There should be an objective or purpose for every component of physical security in how it fits into the overall protection plan. Physical security safeguards are usually purchased in relatively small amounts over a number of years due to budget considerations. There needs to be a road map (plan) to insure that each purchase fits the technical aspects of being compatible with current equipment, product standardization from a cost maintenance and replacement viewpoint, and user buy-in and acceptance. The philosophy of the organization must also be factored in to the direction of the program, i.e., restrictions regarding signage, use of covert CCTV, and the broad issue of restricted versus free access.

CCTV is utilized in many security programs and provides an example of how strategic planning would shape the system. A series of questions will help shape the plan.

- Will the system be centrally monitored or departmentally monitored?
- Will it be used to monitor patient activity? How will those images be monitored?
- Will the system be centrally recorded or departmentally recorded?
- What is the policy or plan regarding the use of fixed cameras versus movement (pan, tilt, zoom) cameras?
- What is the policy or plan regarding covert versus overt camera placement?
- Will the CCTV system be integrated with other electronic physical security components, fire systems, and/or building management systems?
- What is the policy or plan on utilizing “legacy” equipment?
- What other departments inside the healthcare facility will be part of the design and evaluation process?
- Who can determine camera placement and utilization?
- Who is authorized to purchase equipment?
- Who is authorized to release archived images?
- Will equipment be standardized as to manufacturer and/or technical specifications?
- Will equipment be maintained by in-house or vendor arrangement?
- What is the maintenance and equipment replacement schedule?
- What is the optimum size of the system in relation to the total security program?

There should be a business plan approach to the utilization of physical security safeguards. This plan should address the current year and project plans, objectives, and funding for a minimum of 5 years. It is common to divide the plan into short-term and long-term sections.

### Employee/Staff Involvement in the Protection Program

It is universally agreed among security administrators that staff must take ownership in directly contributing to the protection of the organization; however, there are issues beyond practicing good security. One of these issues is the authority for intervention. When security is called to a nursing unit because a patient or visitor is out of control, who is responsible for directing actions—security or nursing? The answer is either one may be appropriate; however, this role should be clear in the strategic plan and protection of the resultant policy/procedure. When there are drugs missing from the pharmacy is this a pharmacy problem with support from security, or a security problem to be resolved by security with support from the pharmacy? When a laptop computer belonging to the organization is stolen, can the employee simply order another one, or does it require a report to security before the purchasing unit will order or otherwise provide a new one? These are the types of strategic questions that must be answered from a strategic context to provide the proper operating fabric and coordinated direction of the protection effort.

## Building Configuration and Design

The most cost-effective security is that which is designed and planned during renovation or new construction. Traffic patterns can be planned and new security hardware can be installed at far less cost than a retrofit situation—some security professionals estimate savings to be a third of the costs. Funding is often more easily obtained when it is included in the total construction package. New construction will often present the opportunity to begin a phased approach for introducing a new system for the whole campus. The best example is that of introducing electronic card access. A system for a large campus could cost in excess of a million dollars or more at build-out. This large expenditure is typically spread over several years. The first phase may be a physician office building with proper strategic planning that includes the basic hardware and software to accommodate the entire campus and all off-site facilities. The strategic plan should stipulate that no construction or installation of security hardware can be purchased or installed without the review, and approval if necessary, of the director of security or the designated person responsible for total organization protection.

## Strategic Plan Unique to Organization

The security strategic plan will be unique to each specific organization as to form, format, and subject area. This plan, however, is necessary for all organizations to provide a clear program direction. Without the framework of strategic security policy and infrastructure, a program simply becomes one of day-to-day reaction, often resulting in a nonproductive and costly effort. The strategic plan, in its final format, affords additional protection as it helps document “the why” behind what is being done in the protection program. In the event of an adverse situation, the protection afforded by this alone is significant. It demonstrates the importance of security to the organization and comprehensively documents all that has been done. It shows that security is taken with importance from the highest levels.

## References

1. Joint Commission Accreditation Healthcare. (2008). *2009 hospital accreditation standards*. Oakbrook Terrace, IL: Joint Commission Resources, pp. 29–30.
2. Joint Commission Accreditation Healthcare. (2008). *2009 hospital accreditation standards*. Oakbrook Terrace, IL: Joint Commission Resources, pp. 44–45.
3. Joint Commission Accreditation Healthcare. (2008). *2009 hospital accreditation standards*. Oakbrook Terrace, IL: Joint Commission Resources, p. 57.
4. Joint Commission Accreditation Healthcare. (2008). *2009 hospital accreditation standards*. Oakbrook Terrace, IL: Joint Commission Resources, p. 74.

# Managing the Basic Elements of Healthcare Security

The function of a healthcare security program goes far beyond simply addressing security risk and vulnerabilities. The program must provide a whole host of services. In this chapter, we will review the basics of healthcare security; the fundamentals that healthcare security administrators can never afford to lose sight of.

Various functions of the healthcare security program must work together to reduce security risks and provide tangible benefits in support of the organizational mission. Each organization must determine how the functional security program elements will be implemented and managed. They may be assigned to different individuals and departments, or they may be brought together under a specific department or division. In this respect, not all elements of a protection system are performed by one department. An example of this concept is the background investigation of applicants seeking employment. The background investigation is an element of the protection system that is generally performed by the human resources department rather than by security.

Security programs must be structured to protect the organization within the restrictive factors of organizational mission, vision, and core values; physical design; patient and community demographics; employee and public relations; budget and resource availability; and the operational requirements of the facility. It is essential to garner an understanding of the culture of the organization. The design of the security program must mirror and support that culture.

The security function should not be applied in such a manner that it is unduly restrictive in terms of the operational efficiency of providing quality patient care. The healthcare security function must be viewed as an element of management that supports creating an environment in which healing can occur. This support will involve numerous systems and subsystems of protective services.

The security function cannot be static; rather, it must continuously evolve to meet the changing needs of society. It must remain flexible to cope with the constant changes in security risks and vulnerabilities that occur in a changing patient-care environment. It must also be continuously evaluated to ensure that the protection function is fulfilling the organization's objectives and needs.

The security function has a different focus, however slight, in each and every facility. Despite this, security practitioners and healthcare administrators agree on one point: the security function must always be rooted with a service orientation and not based on a law enforcement focus. The law enforcement function is designed to provide protective

services from an external or environmental standpoint, and it cannot provide the internal safeguards that comprise up to 90% of an organization's security system—prevention, education, and public relations. Investigations and policy enforcement are important roles of a sophisticated protection program but should not drive the structure and organizational mission of the security department.

Security programs still tend to develop along the lines that reflect the strengths and weaknesses of the person responsible for the program rather than organizational needs. For example, if the responsible person has a background as a firefighter, the protection program will often be structured toward a strong fire prevention and control system. A person with a strong background in investigation will use investigation as the backbone of the program, and the other elements that support this emphasis.

It cannot be stated strongly enough that the organization—not the individual responsible for security—defines the security function. This does not mean that the security administrator cannot craft the security master plan or provide directional input. However, the underlying security philosophies that are put into place by the facility should not be developed in a vacuum. It should include key constituents of the organization to include leadership representatives from the emergency department, IT, human resources, facilities, and risk management. However, in the end, the administrative leadership of the organization must support and give approval—designating the responsibility, providing authority, and allocating the resources necessary to implement the security program.

Protection safeguards for smaller healthcare organizations will vary significantly as to whom is assigned responsibility. In a critical access hospital, protection responsibilities could include the nursing supervisor, plant operations staff, risk manager, the facility administrator, or any combination. In the case of medical clinics and nursing homes, the entire responsibility often rests with the business manager. Less formalized than larger organizations, the assignment of responsibility is often unwritten and vague. One of the inherent problems in smaller healthcare organizations is that employees often have responsibilities for disciplines outside of their experience or educational specialty. No one can be completely knowledgeable in all fields. When one individual must perform many varied tasks, the protection system is often given low priority.

This trend was demonstrated in a stinging report issued in 2008 when investigators for the inspector general for the US Department of Health and Human Services (DHSS) said that the vast majority of nursing homes have been cited for violations of federal safety and health standards. The DHHS report alluded to the absence of effective security processes and procedures and inadequate security investments as issues affecting patient/resident safety.<sup>1</sup>

A security operation cannot be superimposed, like an umbrella, on a healthcare organization with any degree of effectiveness. Rather, it must be integrated into the routine operations of the organization. To produce the maximum return for the investment, security must be a service-oriented entity.

When security officers culturally assimilate to the service philosophy, they become a viable and important part of the healthcare delivery system. The officers themselves develop a better understanding of how protection efforts help the organization meet its mission of

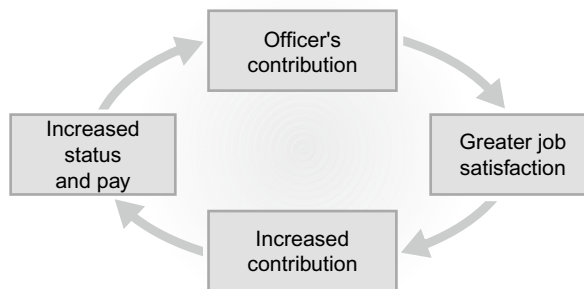
providing quality patient care. When officers understand how their services contribute to an organization, three very important things can occur. First, they find greater job satisfaction. Second, the officer's status is generally elevated in the eyes of the entire organization. Third, as a person or function becomes more valuable to a system, the payment for services is generally increased. All organizations review their program in terms of worth or return on investment. The complementary interrelationship of these factors is illustrated in [Figure 5-1](#).

In general, although security officers perform many customer-oriented services, they also provide a visible deterrent to crime and are available for emergencies if needed. Moreover, in the course of providing services, the officer's interaction with other employees, patients, and visitors is often instrumental in collecting information concerning the protection of the organization that would never have been reported or would not be available elsewhere. In other words, conversations and observations that occur in the course of providing services often yield valuable security information.

A case in point concerned the theft of a considerable amount of money from a medical clinic. As the security officer escorted a receptionist to her vehicle, he remembered that she had previously told him she was afraid her car might be repossessed because she was behind in her payments. Several weeks later, the receptionist told the security officer that she was now current with her payments. An inquiry revealed that the receptionist had in fact made four payments the day after the theft. Subsequent investigation resulted in her confession.

Security administrators do not need much imagination to find ways to be of service to the organization, either in a general way or by specifically supporting a single department. The concept of service can, of course, be carried too far, and one must constantly keep in mind that the security department's primary responsibility is protection. An example of this is the delivery of lab specimens to off-site locations after hours, pulling the only patrolling security officer off-campus and effectively rendering them unavailable for service. However, it is rare for a security program to carry the concept of service within the healthcare organization too far.

The basic functions of a healthcare security program are customer service, maintaining an orderly environment, preventative patrol, incident reporting and investigation, response to requests for service, security communications, parking and traffic control, accident



**FIGURE 5-1** Relationship of security officers' effort to job status.



reporting and investigation, security education and training, applicant background investigation, reaction to internal and external emergencies, enforcement of rules and regulations, access control, liaison with law enforcement and other government agencies, internal and external audits, locks and keys, and a host of supportive services. [Figure 5-2](#) is a listing of the

Ambassadorial Services	Monitor Over 3,000 Alarms
Photo Identification Processing	Bicycle Patrol
Monitor BAPERN Radio System	Intelligence Gathering/Dissemination
Conduct Educational Seminars	Panic Alarm Responses
Monitor Parking Coupons for Volunteers/Chaplain	Surveillance
Medical Assists	Eloped Patient Searches
Victim Services Provider	Disaster Committee Participation
Provide Adverse Weather Condition Dissemination	Conduct Investigations
Hate Crime Information Dissemination	Threat Analysis
Evidence Collection	Maintain Lost and Found
Media Alerts	Community Policing
Arrests and Court Adjudication	Provide Personnel Escorts
Organize Fairs and Special Events	Patient Restraints
Enforcement of Hospital's Alcohol Policy	Standbys for Patients
Off-Hour Delivery of Emergency Organs	Off-Hour Pathology Escorts
Remove Solicitors	Hand Gun Retention
VIP Protective Services	"Code Red" Responses
Monitor Beeper for CODE Call Responses	Key Control
Provide Animal Rights Information	Document Reported Incidents
Draft Department Policies and Procedures	Missing Person Searches
Liaison with Law Enforcement Agencies	Provide Directions
Photographing of Patients	Provide Community Education
Provide Information of Street Closings	Provide Currency Escorts
Fingerprinting Services	Provide Administrative Escorts
Operation ID	Door Openings
Conduct Internal Affairs	Handle Confidential Information
Helipad Responders	Investigation As Needed
Investigate Bomb Threats	Elevator Entrapment Assist
Patient Valuables Assist	Hazardous Material Spill Response
Notary Public Service	Emergency Medical Responses
Dissemination of Departmental Information	Maintain Access Control
Patrol of over 50 MGH/Partners Buildings	Tow Illegally Parked Motor Vehicles
Motor Vehicle Assists	Record Keeping
Phone Referrals	Conduct Security Surveys Incident
A.L.E.R.T. Program	Traffic Control
Crime Prevention Information/Literature	Training
Infant Protection Systems and Response	Mail Service Functions
Code Blue Response	Patient Escorts
Irradiator Alarm Response and Recording	Off-Hours Receiving
Bulletin Board Services	CAS/VPN Delivery
MBTA Monthly Card Distribution	Maintain Taxi Voucher Program
Security Surveillance Rounds	Community Liaison
Maintain Mother's Rooms	Community Policing
Mediation Services	
Critical Incident Counseling Assistance	
Multiple Off-Site Location Patrols, Assists, and Alarm Response	
Monthly Testing: Panic, Elevator Phones, AEDs/Parking Alert Boxes	
Investigate Domestic and Workplace Violence Issues	

**FIGURE 5-2** Listing of security services.

variety of services provided by the Police and Security Department at Massachusetts General Hospital.

## Customer Service

The successful healthcare security program incorporates the principles of good customer service. The historical perspective of security and customer service being polar opposites is no longer acceptable. Today's healthcare environment is heavily influenced by the hospitality industry. Competition is found not only for physicians and patients (customers and consumers) but also internal resources and the talent needed to provide quality patient care (nurses and other allied healthcare professionals).

Often, security officers are among the first people patients and visitors see. They need to create positive feelings about the healthcare facility while enhancing the perception of personal safety for everyone on campus. A simple, yet effective approach is greeting all persons a security officer comes into contact with eye contact and acknowledgment of others is a proven technique for deterring unwanted behavior and activities. The late Sam Walton introduced the concept of greeting all customers at the front entrance of all of his stores and found that the reduction in shoplifting alone more than offset the expense of the position. However, store customers view the greeting as great customer service, not a security procedure. The application of this concept in healthcare is becoming more widely used with great success.

Long-term security program success evolves from a customer-service-focused department. More than just security, staff members are ambassadors for the organization they serve, practicing the rules of customer first and courteous enforcement. Their image, actions, and interactions with patients, visitors, and staff should leave an encouraging feeling about the hospital and the security program. This will include being available to answer questions, providing directions and escort service, and serving a general purpose of being a "walking around" information desk. In general, the uniform presence is symbolic of a person of authority and someone who is in the know. Great customer service and security service blend together for the collective good when helping others find their way. When guests and patients are provided good way-finding and direction, a feeling of goodwill is formed. Persons are able to get to where they are going without confusion and anxiety. From a security perspective, they are not allowed to wander around the facility aimlessly and encounter opportunities for criminal activity that are present in every healthcare facility.

## Maintaining an Orderly Environment

Wherever there are crowds of people, there will be manifestations of disorderly conduct, including destructive and disruptive acts that must be controlled. There is often a fine line between settling a minor incident by handling it internally and having to call for police assistance. A challenging but common example of this is found in the waiting areas for Intensive Care Units (ICU). Families of patients in the ICU are often in the area for

extended periods, distraught about the condition of their loved one and highly emotional. Their expressions are frequently frenzied and unrestrained. Security staff must assist in controlling the environment so that other patients and visitors are not overly disturbed by this type of outburst. In some instances, outside assistance may be needed due to the size of the family and their cooperation with security directives. The underlying issue here is that not all acting out situations occurring in the healthcare environment have a criminal intent. The very nature and purpose of the healthcare organization can elicit many emotions and strong reactions in patients and visitors that are unlike any other environment—a basic element for every security staff member to know and understand.

The function of maintaining an orderly environment relates directly to the other roles of providing patrol and supportive services. The main objective is to prevent incidents entirely or to handle problems effectively when they occur, with a minimum of disruption, harm to persons, or adverse publicity.

## Preventative Patrol

A fundamental security role is the patrol or surveillance of an area to determine that conditions are normal and to serve as a deterrent to negative behavior. This element of protection is not always just the responsibility of the on-site security officer. It can be performed by a variety of different people or processes within and outside the organization. Medical clinics, for example, may rely on police or mobile security patrols to randomly check the exterior of the premises during the night. Hospitals may perform this function by assigning the task to employees: e.g., maintenance personnel in the normal course of their duties, nursing supervisors conducting their rounds, and of course, the security officer on patrol.

Ever increasingly, healthcare facilities are supplementing physical patrol by monitoring images captured through their CCTV system. Conducting virtual patrol through a central command station on a periodic, scheduled basis or as emergencies arise is an effective method to determine that conditions are normal. However, it does not offer the same deterrent to crime and negative conduct as the security officer on patrol. This approach is best applied when a facility is closed or shut down with minimal pedestrian traffic.

## Incident Reporting and Investigation

No security program can be effective without proper reporting of security incidents and investigative follow-up of these incidents. An important factor in reporting incidents is to maintain a simple and easy-to-access procedure. One telephone call should be all that is required of an employee, visitor, or patient to report a security incident.

Trending collected data is important to measure changes in the security environment over time. Analyze monthly and review how reported security incidents trend by day of the week and hour of the day. Compare month over month statistics, year over year data, and seasonal tendencies that affect the safeguarding of a healthcare organization. Use the reports to identify changes in workloads, which may require staffing or deployment

adjustments and as part of the overall annual review of the Security Management Plan per TJC 1. A sample security department monthly report is included in Appendix I.

The industry has not produced a recommended list of incident classifications; however, the list in [Figure 5-3](#) is utilized by HSS Inc. and integrated into the security program at many hospitals in the United States.

A major element of protection is investigation, required regardless of the size of the healthcare organization. In this frame of reference, the term *investigation* takes on a rather broad meaning and is not limited to the initial response or follow-up of a criminal incident. It refers to the collection and preservation of data or materials and the proper analysis of collected materials to manage criminal or civil actions, business situations, and as a basis for protective services programming.

Investigation is necessary for such general purposes as the following:

- To discover the facts and to determine the cause of an incident that may have resulted in loss or possible injury to staff, visitors, or patients.
- To determine adequate procedures and safeguards to manage the various organizational protection vulnerabilities (e.g., to analyze the system of handling patient valuables to ensure safekeeping or to determine whether such handling is designed to minimize the risk of various malefactions).
- To successfully resolve a crime.
- To determine if in fact a crime has been committed.
- To determine the facts and causes of employee work accidents.
- To obtain additional information for law enforcement agencies in cases in which the organization may have an interest.
- To determine the truthfulness of an improper conduct allegation against an employee.

The follow-up that comes from investigations serves many purposes to include physical and psychological deterrence to employees associated with how important the above listed issues are taken within the organization. The prevention of future crimes is an important component of the investigative effort, as investigative follow-up allows for immediate identification of procedure changes that may need to be altered. An example is the office manager who reports a theft of surgical instruments from an unsecured storage area. The investigator can quickly identify steps to take to secure the area and help facilitate the process quickly to prevent a future reoccurrence.

## Response to Requests for Service

The response to requests for assistance is a major facet of a healthcare security program. Some security professionals disagree about the types of requests that are appropriate for security interaction. In most programs, security responds to almost any situation when called on, even though at times it is necessary to refer action to another department or outside agency. Successful security departments have learned that requests for service

**ALARM-ENVIRONMENT**—non-fire and non-security system monitored by or responded to by security

**ACTUAL**—detection of possible or actual event

**DRILL**—pre-planned test of equipment, procedure, or staff knowledge

**MALFUNCTION**—mechanical or electrical problem

**USER ERROR**—human activity not related to an actual event or drill

**ALARM-FIRE**—detection of possible or actual heat, fire, smoke, extinguisher, or water flow

**ACTUAL**

**ARSON**—intentional attempt to burn or actual burning

**DRILL**

**MALFUNCTION**

**USER ERROR**

**ALARM-SECURITY**—a security system monitored by or responded to by security

**ACTUAL**

**DRILL**

**MALFUNCTION**

**USER ERROR**

### **ASSAULT**

**AGGRAVATED**—assault of a person with a weapon or where severe bodily injury occurs

**TO EMPLOYEE**

**TO PATIENT**

**TO VISITOR**

**RAPE**—forcible and unwanted carnal knowledge of a person

**OF EMPLOYEE**

**OF PATIENT**

**OF VISITOR**

**SEXUAL**—any sexual assault other than rape

**TO EMPLOYEE**

**TO PATIENT**

**TO VISITOR**

**SIMPLE**—non-aggravated and non-sexual assault

**TO EMPLOYEE**

**TO PATIENT**

**TO VISITOR**

**AUTO ACCIDENT**—vehicle or property damage or personal injury from a moving vehicle

**PERSONAL INJURY**

**PROPERTY DAMAGE**

**BURGLARY**—unlawful entry, with or without force

**TO BUILDING**

**TO VENDING MACHINE**

**TO VEHICLE**

**CHEMICAL EVENT**—spill or exposure to chemical or fumes which could or causes injury or damage

**CODE ASSISTANCE**—possible or actual emergency or disaster requiring security involvement

**EXTERNAL**—generated by event off campus

**ACTUAL**

**DRILL**

**INTERNAL**—generated by event on campus

**ACTUAL**

**DRILL**

**DISTURBANCE**—personal behavior (not covered in another category) requiring intervention by staff or security

**BY EMPLOYEE**

**BY VISITOR**

**FIGURE 5-3** Security incident classifications.

**DRUG ABUSE**—possible or actual misuse of any drug

**BY EMPLOYEE**  
**BY PATIENT**  
**BY VISITOR**

**FOUND PROPERTY**—property recovered by or turned over to security

**INFORMATION ONLY**—possible or actual event not occurring on property; activity requiring security time or effort to investigate; suspected criminal or suspicious activity; something not covered in another category

**MISSING PROPERTY**—missing or unaccounted for item

**LOST**

**FACILITY PROPERTY**  
**PERSONAL PROPERTY**  
**WHOLE VEHICLE**

**STOLEN**

**FACILITY PROPERTY**  
**PERSONAL PROPERTY**  
**WHOLE VEHICLE**

**UNKNOWN**

**FACILITY PROPERTY**  
**PERSONAL PROPERTY**  
**WHOLE VEHICLE**

**MURDER**—willful killing of a human being

**OF EMPLOYEE**  
**OF PATIENT**  
**OF VISITOR**

**PATIENT ASSISTANCE**—assist or transport of a patient or patient property; search for a missing patient; an against medical advice discharge

**BEHAVIOR HEALTH**  
**ER**

**MEDICAL**  
**PSYCHIATRIC**

**OTHER**

**MEDICAL**  
**PSYCHIATRIC**

**ROBBERY**—physical taking of property from a person

**ARMED**—by threat or use of a weapon

**OF EMPLOYEE**  
**OF PATIENT**  
**OF VISITOR**

**UNARMED**—without threat or use of a weapon

**OF EMPLOYEE**  
**OF PATIENT**  
**OF VISITOR**

**SLIP OR FALL**—event which could or causes injury to a person

**OF EMPLOYEE**  
**OF PATIENT**  
**OF VISITOR**

**SUICIDE**—attempt or actual taking of ones own life

**OF EMPLOYEE**  
**OF PATIENT**  
**OF VISITOR**

**FIGURE 5-3** (Continued)

<b>SUSPICIOUS PERSON</b>	—person not appearing to have business at the facility or acting strangely
<b>CONTACTED</b>	
<b>NOT CONTACTED</b>	
<b>THREAT</b>	—verbal or written expression to hurt, destroy, punish, or intimidate
<b>TO EMPLOYEE</b>	
<b>TO FACILITY</b>	
<b>TO PATIENT</b>	
<b>TO VISITOR</b>	
<b>TRESPASSING</b>	—person refusing to leave the property after being advised verbally or in writing
<b>VANDALISM</b>	—intentionally causing property damage
<b>FACILITY PROPERTY</b>	
<b>PERSONAL PROPERTY</b>	
<b>TO VEHICLE</b>	

**FIGURE 5-3** (Continued)

must be encouraged and handled with efficiency regardless of the inappropriateness of some requests. It is much better to receive some requests that are inappropriate than to receive no requests by the number of people who access the services being offered.

A common performance measurement for hospital security departments is the ability to respond to routine calls for service in five minutes from the time of the original call. In emergencies, many healthcare organizations strive to respond within two minutes or less. These measures are not always practical, based on other activities that may be currently undertaken and the general security staffing. However, the healthcare facility that cannot consistently meet these goals should closely review their on-site security staffing complement for appropriateness to their environment.

## Security Communications

The successful security function will engage the eyes and ears of all employees in the protection program. To capitalize on employee involvement requires an ability to easily communicate with security staff. Ideally, the healthcare worker is provided with a single number to dial for all security-related calls. Answered by a knowledgeable operator who can obtain the name of the person calling, a call back number, and the basic purpose (need) of the call, the operator should have direct communication with the security staff. In larger security departments, this could be a trained security dispatcher, or in some smaller hospitals, the responsibility could fall with the PBX operators. A growing option has been to outsource the function.

Ideally, direct radio communication is used in each option. However, less sophisticated approaches such as cell phones, pagers, and overhead announcements can be used in the security program. In each, it is critical that the caller receives acknowledgment of every call made for security services.

## Parking and Traffic Control

Parking and the control of traffic are basic services required by most healthcare organizations. The degree to which security is involved in parking depends on program development and enforcement needs. In some cases the control of parking is delegated to a special unit of security, an outside provider of parking management service or even to the maintenance and grounds department.

The volume of vehicle traffic entering and leaving the grounds each day produces a significant problem for most medical care facilities. It is the rare healthcare facility that has built enough parking to meet their high volume needs. A parking survey conducted by a Colorado hospital revealed only one hospital in the entire state that thought it had adequate parking to meet its employee, visitor, and staff needs. In general, as most security administrators agree, lack of available parking is a trend that transcends the healthcare industry as a whole, no matter the location.

The need to keep fire lanes open, assist in minor accidents, ensure orderly parking, and protect parked vehicles is a multifaceted task that requires many resources. In emergencies, TJC explicitly requires that healthcare organizations control access in and around the facility, specifically the emergency department.

Many organizations will use patrolling security officers to periodically survey vehicles to determine if the owner has left items of value in open view, windows left open or partially down, doors unlocked, and even keys left in the ignition. The pending results have proven very successful in soliciting greater employee involvement in the hospital's security awareness and theft prevention programs.

In systems where special parking areas are designated, parking decals are a popular means of control. The vehicle decal, which provides ready identification of the owner or driver of the vehicle, is useful in notifying drivers of lights left on, flat tires, damage, or the need to move the vehicle.

Many organizations use security officers to enforce parking rules and regulations and write safe parking reminders for staff as demonstrated in [Figure 5-4](#). In some larger facilities, this can include obtaining special police powers and writing tickets on city streets. Due to the confusing nature of many parking areas, some healthcare facilities will use a mobile patrol officer to help visitors and patients locate their vehicle.

## Accident Reporting and Investigation

Properly recording the facts concerning injury to employees, visitors, and vendors is an essential security function. Employee accident reporting should be the responsibility assigned to the employee's direct supervisor. However, when their efforts are combined with security, a more comprehensive investigation is conducted. The integrity of the investigation is maintained and it helps eliminate false claims. Further, the consistency of having security's involvement in each provides for better data collection that assists with future loss prevention efforts. The employees' supervisor maintains involvement in the



## SAFE PARKING INFRACTION



Parking in the prescribed manner is an act of consideration for others.  
Your vehicle is parked in violation of facility regulations.  
Vehicles are subject to being towed at Security Officer's discretion.

<input type="checkbox"/> Not in authorized space <input type="checkbox"/> Occupying reserved space <input type="checkbox"/> Loading zone <input type="checkbox"/> Prohibitive sign posted <input type="checkbox"/> Handicap zone	<input type="checkbox"/> Occupying more than one space <input type="checkbox"/> Sidewalk blocked <input type="checkbox"/> Driveway blocked <input type="checkbox"/> Fire zone <input type="checkbox"/> Other _____
--	--

Vehicle Description	License # and State	Permit # (if Employee)	Location
Issued by	Date/Time	Facility	

**FIGURE 5-4** Safe parking reminder.

reporting procedure and typically has responsibility for any follow-up action that may be required.

The security officer should also be responsible for investigating and recording visitor or vendor accidents. Many unnecessary claims have been paid because an accident report was not filled out or because of an incomplete investigative report. Organizations sometimes fail to assign this responsibility specifically. When it is everyone's responsibility, it often ends up being no one's. Without proper records it can be extremely difficult to defend a case in which the plaintiff has all the facts and the organization has no facts or incomplete facts.

## Security Education and Training

A major element of a successful security program is to stimulate, educate, and motivate employees to be conscious of protection needs and to practice good security awareness. Personnel must be trained in the proper response to aggression management, infant abduction, bomb searches, evacuation procedures, workplace violence, and taking ownership in their security responsibilities. In small medical clinics, this function is rather informal and spontaneous; in larger facilities, a more formal approach using many different communication media is necessary.

Presentations, handouts, events, and training will raise staff awareness of security issues. Not only will this add eyes and ears to your security efforts, but it also will be noted by TJC surveyors, who are increasingly looking for employee involvement in security. Using input from your staff, physicians, visitors, and patients, the security awareness offering should be tailored for your facility, and include such activities as:

- Department-specific training on topics such as infant security, aggression management, and Emergency Department security.
- Brown Bag Workshops on crime prevention and personal safety.

- Security fairs.
- Security brochures: These can be custom creations by the facility or generic purchases from the National Crime Prevention Council or other outlets.

Organizations are taking on the broader task of helping employees to be safe and secure outside the workplace. Classes on self-defense, identity theft prevention, home safety, and other topics are offered as an employee benefit on the premise that security awareness must constantly be reinforced.

Promoting security awareness among patients and visitors is also an element of security. Visitors and patients often are victims of various crimes, many of which could be prevented through safer practices. Using signage and other subtle reminders is a good security practice. A few examples are signs in parking areas reminding patients and visitors to secure their personal belongings in their vehicle or admissions staff encouraging patients to send their valuables home with loved ones.

## Applicant Background Investigation

Investigating prospective employees is generally the responsibility of the Human Resources department or, in small organizations, the person who actually hires the employee. Verifications usually entail criminal record searches, citizenship requirements, employment verification, social security number confirmation, and required education and license validation. Some organizations often rely on security assistance when considering an applicant for a sensitive position, such as cashier, pharmacists, child-care services, or home health worker. Typical services often include conducting a worker's compensation claim review, multiple state criminal history review, sex offender registries, Department of Motor Vehicles history report, or simply contacting the Drug Enforcement Agency (DEA) to ascertain knowledge of past incidents.

Laws are constantly changing to meet society's evolving needs and expectations, but so is technology and wrongdoers' capability to produce false credentials and diplomas. Almost every healthcare organization has been presented with this issue and must take it seriously. Consistency in the process of background investigations is needed as the theory of negligent hiring is litigated often and with substantial awards. Hiring an individual without investigating the person's background or improperly placing an individual in a position that requires higher levels of expertise than the applicant possesses are often cited as reasons for verdicts against an organization.

The courts have ruled that employees who have contact with members of the public (i.e., healthcare workers) are held to even higher standard of reasonable care in terms of hiring. This requirement is imposed because it is reasonably foreseeable that such an employee could cause an unreasonable risk of injury to the public.

## Reaction to Internal and External Emergencies

One of the most fundamental concerns within a healthcare facility is the ability to manage properly and swiftly serious emergencies. This requires the ability to react to the

unexpected and to minimize the negative impact caused by noncriminal emergency situations. Frequently, this requires the ability to manage access into the facility. The speed in which access to the facility can be restricted is a key indicator for facility readiness to many internal and external disasters.

The procedure should be tested regularly to evaluate capability. System testing should occur at three in the morning, in addition to three in the afternoon when staffing in the facility is at its peak. It should also assess the time it takes when security is engaged with other activities such as a patient watch or a fire drill.

Other types of internal or external emergencies that concern security are fire and explosions; flooding or severe weather that causes property damage or injury; chemical spills and other hazardous situations; loss of power, water, or communication; and isolation from the rest of the community in a disaster situation.

## Enforcement of Rules and Regulations

The enforcement of organizational rules and regulations is generally considered a security function. This role, however, should not be isolated from the supervisory authority and responsibility throughout the organization. In facilities with an established security force, the operating department's supervisory responsibility is often de-emphasized; as a result, security is looked to for enforcement. This is a mistake. It forces security personnel into a potential adversarial relationship with other employees and visitors. A good example is the policy of prohibiting smoking on campus. Even though the security force acts to ensure compliance on campus, the job should not rest solely with security. It requires the support of and enforcement by every supervisor and administrator of the organization.

## Access Control

Access control, arguably the most critical aspect of healthcare security, requires blending facilities management, mechanical and electronic technology, and good security practices. It is the central role of security to mix each together for a cohesive security system.

While many statistics point to a rather dire state of society, the hope for better healthcare workers' protection can begin with facility management/design. Today's older designs are too open and allow too much accessibility to walk-in guests without any kind of record or accountability. The proper channeling of visitors and patients into and about the healthcare facility is good security and a good business practice as well. The goal is to allow patients/visitors to move freely without feeling oppressed while protecting patients, visitors, and staff.

Today's technological advancements in access control enable higher degrees of security without compromising aesthetics, customer service, user-friendliness, or overall hospitality. Access control can protect critical areas such as pharmacies, surgery rooms, infant treatment rooms, technology closets/rooms, information storage rooms, and areas that separate staff from the public.

In some larger hospitals in downtown, higher-crime locations, access control is tightly administered 24 hours per day, with various checkpoints for visitors, vendor logging and badging, and employee identification systems. In some facilities, restricted access is instituted only during night hours by locking certain doors and channeling access to the facility through designated points. Commonly described as the single greatest risk facing healthcare today, all facilities with inpatients and 24-hour emergency medical service must restrict after-hours access. Controlled through one or more designated entrances, the process must channel visitors so that their presence is acknowledged and a visitor's badge issued. During the process, time should be taken to call the unit to be visited and inform staff who is coming. A common misgiving for hospital staff working at night is coming across a stranger walking around the department and having no idea who he/she is or why he/she is there. A negative perception of personal safety is created with staff and greater opportunity is presented for crime against the hospital to be committed.

The management of this risk is further challenged with many operating philosophies prevalent in healthcare such as those promulgated by "Plane-Tree" and other management philosophies. Offering this open and inviting environment does not eliminate the responsibility to protect patients, staff, and visitors; on the contrary, it only changes the dynamics in how this is accomplished.

## Access to Locked Areas

All protection systems use locked doors to preserve the integrity of a given office or work area. Likewise, all efficient organizations must provide a system to grant access to the areas under special circumstances. The term *special circumstances* underscores the need to control special areas and to provide services to people who require legitimate access but do not have a key, access card, code, or other lock-release device.

Because providing access to locked areas is generally considered to be a security function, certain controls must be established to prevent the security officer from becoming an errand runner. People who need frequent access to a given area should be provided with a means for such access. Basically, the security officer is called on to grant special access to areas that require a high degree of control, such as storerooms, medical records areas, libraries, equipment rooms, and other places where a record of entry is required.

Access to locked areas can also be achieved by holding keys in a central area to which those who desire entry must report to check out the required key. This function can be managed by the security department who can either issue the key or respond to calls for assistance with the key. Many facilities are incorporating secured key closets that provide a specific electronic audit trail. Thus, keys are distributed only to predetermined authorized personnel who use a unique personal identification number to access a specific key. This works especially well in organizations that are challenged with their key control program for designated high-risk areas.

Efficiently granting access to authorized individuals is a service that improves the overall efficiency of the organization. People lock themselves out, mislay, lose, and forget

keys frequently. The security department should provide quick response, so that the necessary work of the organization can progress without undue delay. If these requests appear too frequently, the problem should be handled administratively, not through a delay of service.

### Access to Employee Lockers

A greatly appreciated security service is providing access to lockers when an employee does not have a key or forgets a combination. This service eliminates the need for employees to break into their lockers when they have misplaced or forgotten their locker key. In some programs, a key that will fit only the specific locker is temporarily checked out to the employee. In others, the security department uses a master key to enter the lockers. Where the master key is used, the key should not be checked out to the employee; instead, the security officer should provide the access.

## Liaison with Law Enforcement and Other Government Agencies

All organizations, regardless of the sophistication of their security effort, eventually need to call on local law enforcement and other government agencies. The medical facility must be able to work effectively with many different agencies. It could be the DEA when an issue of drug diversion or theft occurs; local law enforcement for coordination of emergency response plans for natural or manmade disasters; the Secret Service if the President or other political dignitaries visit the region; or the local fire department for evacuation planning and life safety code compliance. The list can go on and on.

Establishing public-private partnerships is more important today than ever before. Chief Harry Dolan of the Raleigh, North Carolina, Police Department commented at the International Association for Healthcare Security and Safety's 2009 Mid-Winter Seminar that building relationships with local law enforcement and other governmental entities is critical to the success of the healthcare protection program. Chief Dolan shared with the audience that hospitals and complex medical centers are often quite foreign to these agencies. Arranging for tours, getting their involvement in policy and procedure development, and general networking were keys to establishing successful relationships which he called critical to liaison efforts.

Outreach efforts are often best handled by the leader of the security department with emphasis placed to coordinate frequent information exchanges. At the Anschutz Medical Campus in Aurora, Colorado, the security leadership at Children's Hospital, University of Colorado Hospital, and University of Colorado Health Sciences Center meet every other month with the local police department and fire department as part of the campus-wide Security Council. Discussing items such as security incident trends and challenges, future large-scale events on campus, new high-risk services, emergency preparedness and exercise planning, and campus-wide policy creation, these meetings have obtained involvement and

shared knowledge that has had a positive effect of the overall protection posture on campus. All parties have a better understanding of their role on campus and have fostered an excellent relationship in the process, each of which pays great dividends in a time of need.

The role of security should never be to supplant the police, but rather to supplement and assist them. As the criminal mind becomes more sophisticated in its approach to wrong the public and specifically the healthcare industry, protection efforts require a coordinated approach with local law enforcement. A successful security program cannot operate in a vacuum.

## Internal and External Audits

Another important function of any protection effort, and one that is often neglected, is to test the procedures designed to protect the organization against such malefactions as internal theft or fraud. Many fraudulent schemes have been discovered by spot checks and internal audits.

There are basically three kinds of internal audits. The first is an unannounced inspection of a procedure. An example would be to check the patient personal property envelopes that are being held for safekeeping to determine that all are accounted for in accordance with the system (i.e., serial numbers properly listed, inventories as required, double signatures for deposits).

The second type of control involves spot-checking incoming or outgoing goods to determine whether the records match the actual commodity. One example would be to randomly compare food delivery requisitions with what is actually delivered. Another would be to measure the fuel oil delivery before it is transferred to facility storage tanks.

The third type of check involves the use of an undercover operative to monitor a service to determine whether correct procedures are being followed. An example would be to determine whether a cafeteria cashier rings up the proper amount, especially after a customer pays the exact amount due. Security operations are also subject to audit and should receive the same review and scrutiny as other areas of the organization.

### External Audits (Inspections)

Many systems are used to keep our healthcare facilities safe. But one of the common missing components is the routine testing of these systems. An external audit is a survey that is concerned mainly with the hardware of the protection system.

At periodic intervals, locks should be inspected, external and stairwell lights checked, CCTV cameras verified that they are capturing the correct image, emergency communications validated to be working, and alarm systems activated to ensure that they are operating correctly. Systems or components found to be ineffective, not working as originally intended, and/or not meeting current needs create undue risk for the healthcare facility. Many electronic security technologies provide automatic system checking to ensure systems are operating properly. There is a need, however, for visual inspection of

security elements such doors, windows, external lighting, fencing, and shrubbery control (maintaining sight lines).

This documentation and testing may be considered small and routine. However, its importance is found in the liability protection afforded to the facility and more prominently, the positive perception of security and the department.

A strategy that works particularly well is to assign someone on staff who, at least on a monthly basis, takes an inventory of all equipment in use, verifying its operational status. If equipment is found missing or not operating as originally intended, document those issues and place them on the internal work order plan to correct the deficiency. When followed, this close-the-loop system ensures systems are working and ready when needed.

The external audit should also include management of the perception of the security program. A negative opinion of security is created when system components have wires dangling or dust build-up. This can include the image associated with damage on a security patrol car. The protection program must mind itself with the symbolic message the ongoing maintenance of security equipment signals to employees, staff, patients, and visitors about how serious security is taken, not forgetting the deterrent signal sent to the bad guy as far as security readiness and the organization's capability to provide protection services.

## Locks and Keys

This protective function is perhaps the most neglected security safeguard, even though it is one that most facilities rely on quite heavily. It has been observed that it is not uncommon for a new lock-and-key system to be out of control within days or weeks of the installation. The control of locks can effectively compel strict adherence to the program. Today, electronic access systems have replaced many locked access points; however, healthcare organizations will always have the need for keys. The issuance of keys at all facilities must be closely tracked and carefully controlled to prevent system breaches.

## Other Support Services

In addition to specific responsibilities, security must also provide support to the various departments and sections of the healthcare organization. Chief among these supportive activities is customer service—giving directions and helping people, especially patients utilizing the facility. Other examples include accepting and properly storing shipments when the receiving department is closed, monitoring blood bank refrigeration temperatures, and escorting cashiers. The list can be exhaustive; however, the important point is that security should provide as many supportive services as possible as long as they do not interfere with security's primary protection responsibility. Security is a service organization, and service is a prime consideration when calculating security cost-effectiveness.

## Lost and Found

Lost and found activity is usually a component of the protection system. The lost and found service benefits the entire organization and is of specific value to the security

program. Although lost and found is operated as a service, it can contribute directly to resolving reports of stolen property. An efficient system of handling found property can clear up many instances of property loss that are reported as theft. Whenever property is missing in a busy medical facility, there is always the question of whether the item was lost, accidentally discarded, inadvertently taken by another person, or taken with the intent to deprive the rightful owner.

Careful review and investigation into each reported loss may often result, for example, in finding dentures and eyeglasses in dietary waste containers as they are frequently left on food trays. Instituting a specific property retention policy, typically 90 days, helps manage the volume and storage of found items. Many healthcare facilities turn over items of value to the local auxiliary for their fund raising and/or goodwill efforts.

The public and employee relations fostered by an efficient lost and found system are of tremendous value to any organization.

## Conservation

Helping to conserve resources is a security function that goes hand in hand with support services and preventative patrols. Utility costs have made saving energy everyone's job in the medical care facility. Security officers on patrol can shut off and turn on lights at specific times, switch off coffee pots or other small appliances unintentionally left on, close windows left inadvertently open, report water leaks, manage temperature settings for meeting rooms, and report equipment that is not functioning properly.

## Deceased Patients

Security involvement in handling deceased patients and their property can be found in numerous hospitals and long-term care facilities. This involvement may include safe-keeping property, assisting in transporting bodies to the facility morgue, granting undertakers access to the facility, and releasing bodies to the mortuary. Although such tasks are generally considered unpleasant for the security officer, one or all of the assignments are appropriate security program responsibilities. Specific protocols should be established providing guidance on credential verification and proper release procedures. When assigned responsibility, the security officer must verify the correct body before releasing the body to prevent an embarrassing and potentially libelous situation for the hospital. For example, a southern California hospital settled a claim to the estate of a deceased patient who was released to the wrong mortuary after the body had been harvested for tissues and organs against the patient's stated desire.

The loss of deceased patients' property is a problem familiar to most security administrators. The question often arises of whether the disappearance of property occurred before or after death. In some cases, relatives or visitors have removed property from patients as they lay helpless. The blame for the missing property is easily shifted to the facility by the family. Of course, one cannot always place the blame for missing property on the relatives or friends of the patient; many cases have been resolved by ascertaining that a hospital employee was responsible.



Although it is common practice, it cannot be stressed enough that a complete inventory of all of the deceased's personal property should be made by two persons as soon as possible after the death. In some programs, this inventory is completed by the security department with a nursing staff witness, and the property is removed for appropriate storage until it can be properly released.

## Patient Valuables

Most every healthcare facility has a policy in place that addresses patient valuables and clothing that include an inventory list to catalog patients' belongings. A common element is to have admissions staff encourage all patients coming to the facility for scheduled appointments or treatment to leave their valuables at home. However, there are many instances when this is not feasible—unscheduled treatments or visits (e.g., visits to the emergency department) or patient refusal to cooperate with the request. In these instances, the security department is often involved in collecting, inventorying, and storing patient valuables.

This patient involvement activity requires the healthcare security program to have processes in place to obtain a complete description of all items collected and the creation of a secured storage process that cannot be accessed without two people (double lock-and-key system). Many organizations attach the patient's bar code label on the tamper-proof storage container and insert the inventory contents page inside to prevent unwanted tampering.

Upon discharge, security officers are often asked to return stored items to the patient. Verifying the contents with the patient against the original inventory prevents future disagreements and confusion.

## Emergency Messages

Relying on emergency messages is a necessary activity of any organization. For the most part, relaying of messages is handled within the normal operating framework of the system. There are, however, important messages that must be properly handled after normal business hours and outside the routine system. An example may include telephone calls to locate employees or visitors to advise them of emergency situations. The security department can and should provide any assistance possible in helping to locate persons and to expedite this relay of important information. The increased use of cell phones and other electronic communications devices has drastically reduced the need to relay messages through security services.

## Cash Registers

The handling of cash is a problem for most organizations. According to the accounting firm of Ernst and Young, of all cash fraud techniques, cash taken by the failure to record sales accounts for about 30% of all losses.<sup>2</sup>

The security department can lend support to the accounting departments in several ways. First, cash registers should be read and cleared by a person other than the person

handling the transactions. This poses a problem for many accounting departments because a number of registers must be cleared at various night hours and on weekends. In many cases, the security department is already responsible for providing escorts when the money is transported to the main vault or cash-holding areas. It is a simple matter for security to provide the additional service of clearing the register and forwarding the tapes directly to internal auditing or another previously designated department.

Without such a system in place, a large medical center in Dallas, TX, experienced all of their parking attendant cashiers working in collusion and circumventing the internal controls in place, costing the hospital over \$1 million in lost receipts in a 4-year period.

A word of caution concerning cash escorts: the security officer should be just that—an escort. The officer should not be the sole transport unless proper tamper-proof controls have been instituted. The route from the cash collection point to the holding area should be varied just as patrol patterns should be varied.

## Emergency Shipments

A valuable support service is the receiving, signing for, and proper disposition of equipment and supplies that arrive at the facility after normal business hours. It is sometimes impossible for a critical shipment to arrive before the regular receiving area closes. In this case, the security department can provide a valuable helping hand to the materials management department.

Clear guidance must be established concerning this support service. Otherwise, outside delivery personnel may not make the effort to deliver on time because they know that security will accept the late shipment. They will deliver first to organizations that do not have after-hours receiving. It is thus important to perform this service on a prearranged request from the materials management department. It should be recognized, however, that flexibility must prevail because it is important that a critical delivery not be refused due to a breakdown in the prearrangement procedure.

Specific handling instructions should be recorded in the system used to pass on information so that all security personnel will be aware of the proper handling of the goods received. At the time the delivery is actually accepted, an entry should be made in the daily activity record indicating the time the delivery was received and where the property was taken for storage.

## Package Check

It may be desirable to maintain a checking service for employee property brought into the facility. Not only does this service discourage organization-owned property from being added to the employee's personal property, but it also provides better protection for employee property than storage in a department. In addition to the security aspects, the environmental services function is enhanced when personal suitcases, packages, boxes, and so on that do not pertain to the departmental responsibilities are stored elsewhere.

This system is quite common in department stores, where packages held by security are released as the employee leaves the building. Already practiced in some healthcare facilities, this procedure requires a firm, consistent policy prohibiting the employee from taking certain personal property to his or her work area.

### Distribution of Reports and Equipment

In one hospital, the daily census report prepared by the admissions office is distributed each night by a patrolling security officer. Previously, the admission employee was responsible for this task, which required approximately 30–45 minutes. Because only one admissions clerk was on duty at this time, the admitting function was left uncovered. The security officer frequently found people who needed admissions services wandering around. The security administrator determined that it would serve the best interests of the facility from a protection standpoint if the security officer distributed the report. While providing this distribution service, the officer also conducts a patrol of the area. Because the reports are not always ready for distribution at the same time each day, the patrol round occurs on a no patterned basis.

The problem of providing wheelchairs at the proper time and place where needed occurs in all facilities, regardless of size. Although this need is predictable to a certain degree, employees frequently need to search for a wheelchair. The continuing need for wheelchairs defies real control, and it is generally impossible to determine the location of wheelchairs at any given time. An added complication is the fact that patients' private wheelchairs are often brought to the facility. Most security operations can cite examples of missing patient wheelchairs that took days to find after an employee inappropriately used the chair to transport another patient.

In one program, all unit location markings were removed from the chair and a standard was prepared that specifies the number of wheelchairs that should be in a given location. According to this standard, during the late-night shift, the security department was responsible for redistributing the wheelchairs.

### Flag Etiquette

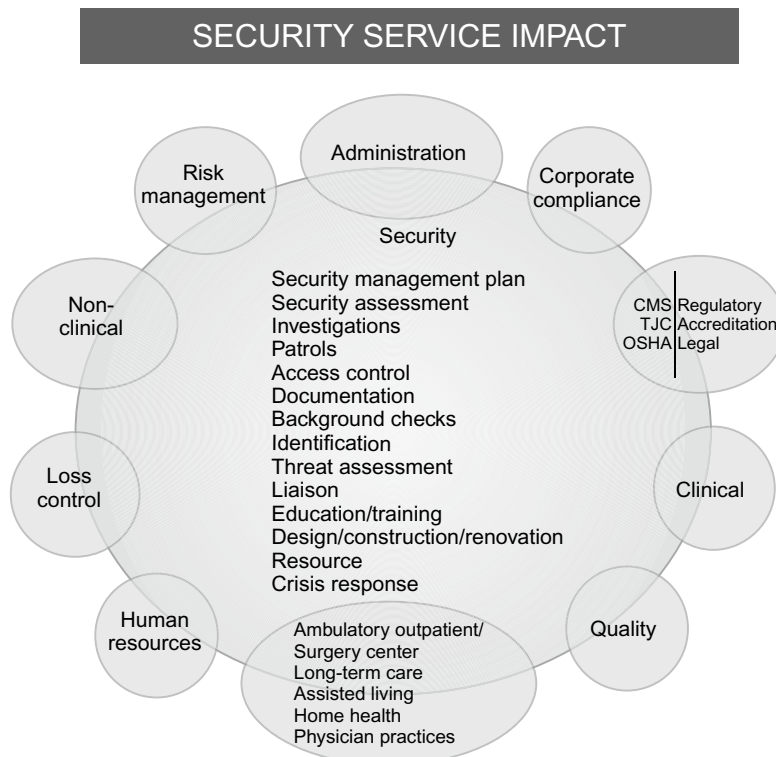
It is not uncommon to assign the task of raising and lowering flags to the security department. Security officers, especially those in uniform, add a certain dignity to this activity. Although this function is strictly a service, it is one to which even security administrators who oppose the service concept can seldom raise a suitable objection. In one hospital, the security department not only takes great pride in handling the flag etiquette, but also buys the American flag for the facility through donations from security personnel. It is, however, common to continuously fly the flag with night lighting.

### Miscellaneous Services

The number of security services is almost endless. Services should be implemented only if they fit into the system without jeopardizing the basic protection function. Some

miscellaneous services other than those previously listed may be found in specific programs. One of these is turning equipment on or off. This may be a routine service, such as turning on kitchen equipment before food service employees arrive, or the specific environmental control of a researcher’s experimental project. Another service is providing storage for firearms belonging to patients. Controlling valet parking areas and interacting in facility transport systems is also a frequent role for security departments. In one hospital, the security officer records the number of people using hospital-controlled buses to provide important operational planning data. Another service frequently requested of security officers is helping with patients.

Services are limited only by the needs of the organization and the imagination of those in charge. Security administrators who continually object to requests because “that is not a security function” may only be reflecting their narrow view. One must always remember that security is part of the healthcare team and patient needs are paramount. Figure 5-5 presents a diagram of the various healthcare security service activities and their organization impact.



Copyright © 1998 by Safety And Security Solutions, L.L.C. All rights reserved.

**FIGURE 5-5** Basic healthcare security service activities and functional organization impact.

## Public/Employee/Community Relations

The security effort is created to serve the healthcare organization. The organization is people—all sorts of people, including visitors, employees, patients, physicians, vendors, delivery people, repair technicians, researchers, and students. The overall security program must be accepted and understood by the organization it serves. Security personnel must exhibit a helpful and friendly customer service attitude toward everyone they meet. In many instances, the security officer is often the first and the last person that a patient or visitor to a healthcare facility meets. The image projected by the officer can set the tone for the person's feelings toward the organization. Security cannot operate in a vacuum and must function as part of the team in providing quality patient care.

## References

1. Solutions by market special publication—healthcare. (2008, November). *SDM Magazine and Security Magazine*.
2. Gerboth, D. L., Hoenecke, J. B., & Briganti, R. (1989). White collar crime: Loss prevention through internal control. *Chubb Group of Insurance Companies*, 8.

# Security Department Organization and Staffing

A well-trained and properly supported (financially and administratively) security force is the basic component of the healthcare protection system. Although the security staff is the backbone of this effort, it is perhaps only 20–25% of a well-rounded security and productive security system. A successful security program must also include basic components of positive security contributions of facility staff, full support of administration, including financial resources, and effective physical security safeguards. In fact, in some small facilities, there are successful security programs in which there are no security personnel; however, there must be a 24/7 designated security force response capability. In these cases it may be that the maintenance staff (or other organization personnel) assume certain security duties and responsibilities. Regardless of facility size, or the size of the security force, there must always be an integrated approach with the other organizational resources that contribute to a successful cost-effective protection program. The achievement and the ongoing management of this integration are the direct responsibilities of the security program administrator.

## Security Function Reporting Level and Support

The security function serves, supports, and is interrelated to all aspects of the healthcare organization. As such, security is considered an element of administration. A required component of the Security Management Plan is to clearly specify the position that has the responsibility for security of the organization and has a clearly defined reporting level for this position. The hierarchical level in the organization to which security reports reflects the importance that administration places on the security function, and the organization's responsibility of protecting persons and property.

It has been argued by some security practitioners that the security function must report only to the chief executive officer (CEO) or the chief operating officer (COO). This may sound good in theory, but it is generally neither practical nor a satisfactory situation. The basic problem is accessibility. Both the CEO and the COO are performing functions that, by necessity, do not generally involve day-to-day nonclinical department operations.

On the other hand, the security function must not report at a level that negatively affects its productiveness. The security function, like many other functions in healthcare, has been a victim of organizational “flattening out.” The various management levels in healthcare organizations that once existed are gone. As a result, security has often

been pushed lower in the organizational hierarchy. The important aspect of the security reporting level is that it must provide the organizational authority necessary to properly carry out its mission. A practical consideration is that security should report to an individual who has both the time and interest in the security function. In short, there must be proper administrative support for a program to be effective and productive. This reporting level must have sufficient stature to carry the ball when a decision is outside his or her realm of direct authority or when information of a sensitive nature must be communicated to others at higher levels within the organization.

A common reporting level for security is the vice president (or director) of facilities or the risk management administrator who, as a generality, seems to fit the foundation criteria for a successful program. Likewise, other highly successful programs report to the vice presidents of finance, human resources, and administration. Regardless of the reporting level, the professional security administrator must be cognizant of the organizational support level cycle. The concept of the cycle is that at critical times security is a top priority of the organization resulting in a high level of support for security in terms of funding and philosophy relative to security policy and procedures. At other times support may be practically relaxed to a routine operating level where there is minimal day-to-day support. Dennis Dalton, in his book *The Art of Successful Security Management*, suggests that the support cycle consists of three phases: strong organization support, confusion, and a lack of support.<sup>1</sup> In Dalton's support cycle, the confusion stage is one that can sneak up on the security administrator. This confusion cycle can occur when the program is running smoothly and there is little or no perceived security threat. It is a time that management and staff feel safe and may be totally focused on other management and patient care issues.

There are various signs and clues that will alert the security administrator that the program has entered or is entering this confusion stage of the support cycle. Chief among these signs are:

- A general indifference toward the program by top management and a lack of understanding of the duties and activities of security that contribute to the healthcare mission.
- Advertent or inadvertent exclusions from meetings where issues clearly entered into the area of protection.
- Planning of activities or events with security implications without security involvement.
- Department heads and supervisors make assumptions about the security program without seeking clarifications or confirmation of program components.
- Decreasing ability to influence or have a voice in sanctions relative to internal misconduct situations.
- Increased staff disregard for compliance with security safeguards, policy, and procedure.

In the third stage of the support cycle there is outright rejection of plans and programs, top management avoids security input or discussion, and staff shows little support for the security function. This is a critical time for the security program and the

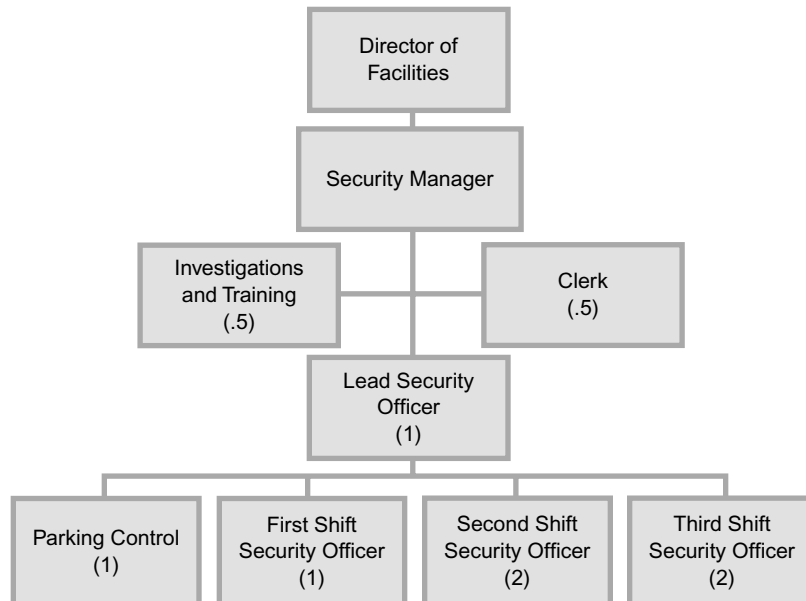
security administrator who must do all possible to end this final stage of the cycle and return to the full support phase. Failing to accomplish this objective indicates a time for a change in security leadership.

## The Functional Organization Chart

In essence the administrative plan for the entire organization is recapped in the functional organization chart, which defines the relationship of the components of the organization. This chart further establishes the chain of command. However, the chart specifies only formal authority relationships; it omits the many significant informal relationships. Further, it does not generally indicate the degree (limits) of authority that exists at any point in the organizational structure.

The organization of a security department is limited only by the imagination and desires of the person responsible for the protection system. Organizational charts range from simple to complex. Each facility or organization has its own format, style, and procedure for preparing the department organization chart. The charts in Figures 6-1 and 6-2 are offered as examples of actual working charts in the single stand-alone facility. They are not intended to be used as models as each protection program is unique in scope, function, reporting level, and budgetary realities.

As shown in [Figure 6-1](#), there is an allocation of 0.5 FTE for Investigations and Training and 0.5 FTE for an Administrative Clerk. There are several ways these two positions of 20 hours per week each could be staffed. A part-time administrative clerk that could work a 6-hour shift 3 days per week (M-W-F) would be ideal. This staffing arrangement would allow flexibility in utilizing the additional 4 hours per pay period (2 weeks) where most needed.



**FIGURE 6-1** Example of a small security department organization chart.



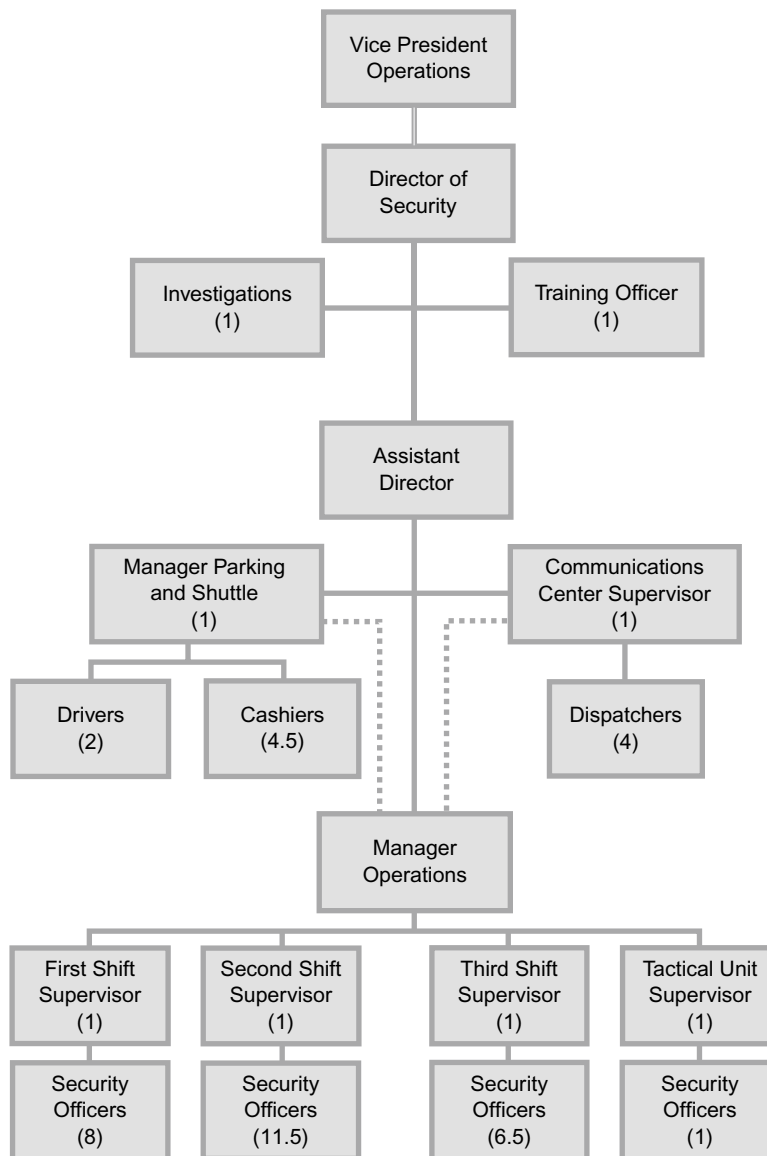


FIGURE 6-2 Example of a large security department organization chart.

The investigations and training officer could be staffed by a senior security officer working at such two 8-hour shifts per week and filling in a regular officer duty shift three times per week. A limited amount of investigative and training activity could also be accomplished during regular duty shift time. In short, the deployment plan is left to the creativity of security leadership balanced with the specific protection needs of the health-care organization.

## Healthcare Systems

The organizational chart and the delivery of security services in large healthcare systems created by mergers, buyouts, and affiliations may look quite different from the stand-alone facility. The various facilities in a system are often located many miles apart in the same service area or even in multistate locations. These healthcare systems develop their own specific management operating philosophies, and these philosophies range from centralization to quasicentralization to decentralization with variations of form in between.

### *Systems (Multifacility) Security Management Control*

There are various levels of systems management that can be used to achieve standardization of protection services, increase the quality of performance, and provide a favorable impact on budgets. These levels range from an informal working group of security managers from each facility to a full corporate system administrative and operational control responsibility. The benefits can be optimized by a total centralized system management approach; however, it is the most difficult to achieve, due to many factors including individual facility philosophies, turf control issues, staff personal prejudices/biases, organized labor issues, and individual facility ability to fund their share of the program and the reality of geographical distances.

In the complete centralized philosophy approach there is one budget with full line authority to operate a consolidated systems program. There may be some internal cost accounting allocations of facilities being served but from an operations standpoint each facility would receive security services as a one-campus approach, even though facilities, or sites, may be miles apart. Rarely is the total centralized security system model used when facilities are located in multistate locations.

The quasicentralization philosophy, which is the most popular, generally operates within a given metropolitan area via a central corporate budget and facility-specific budget for security. In this approach the central office may provide support functions such as training, investigations, consultation, and documentation including TJC compliance, strategic planning, equipment standardization including maintenance contracts, and often a central communications monitoring center. In some programs the central office would also provide for a common external grounds patrol and/or a consolidated patrol/field supervision approach. In this methodology the patrol field supervisor will often represent the authority of the facility security manager during evenings, nights, or weekends. Also, in this approach security staff for individual facilities are generally hired by the individual facility manager and usually paid as an employee of the individual facility. The facility manager would report to the central (corporate) director and be paid through corporate funding. This presents a contract management concept for the facility; however, this corporate facility security supervisor would work very closely with the facility administrative person responsible for the security program. In other cases, the facility security supervisor may be an employee of the facility and have a “soft” reporting relationship to the corporate security hierarchy.

In the completely decentralized approach each facility maintains complete control of their security effort with no line authority outside of the specific facility. In this

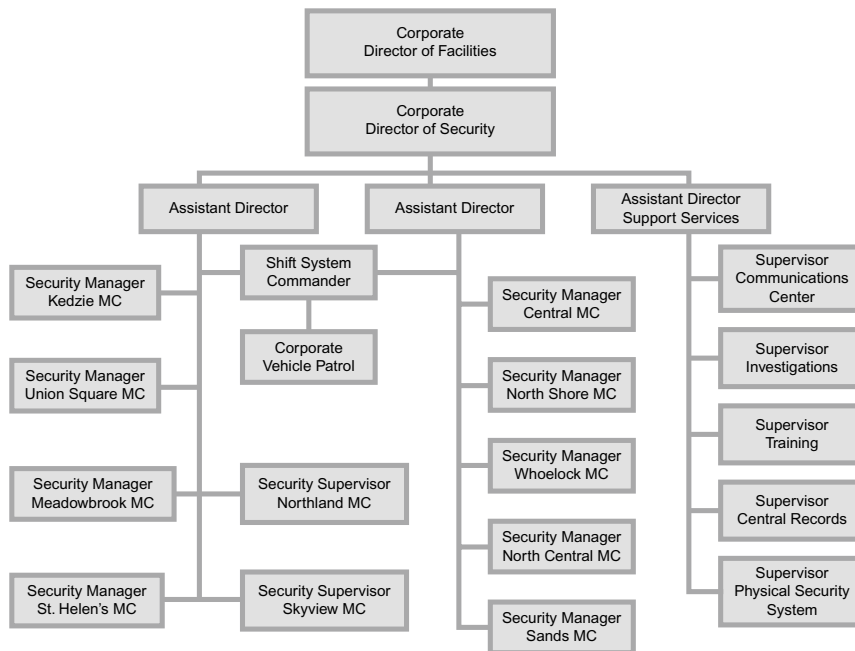


FIGURE 6-3 Example of a healthcare system corporate security organization chart.

approach there may be a centralized corporate security support function; however, this function would generally only be advisory in nature.

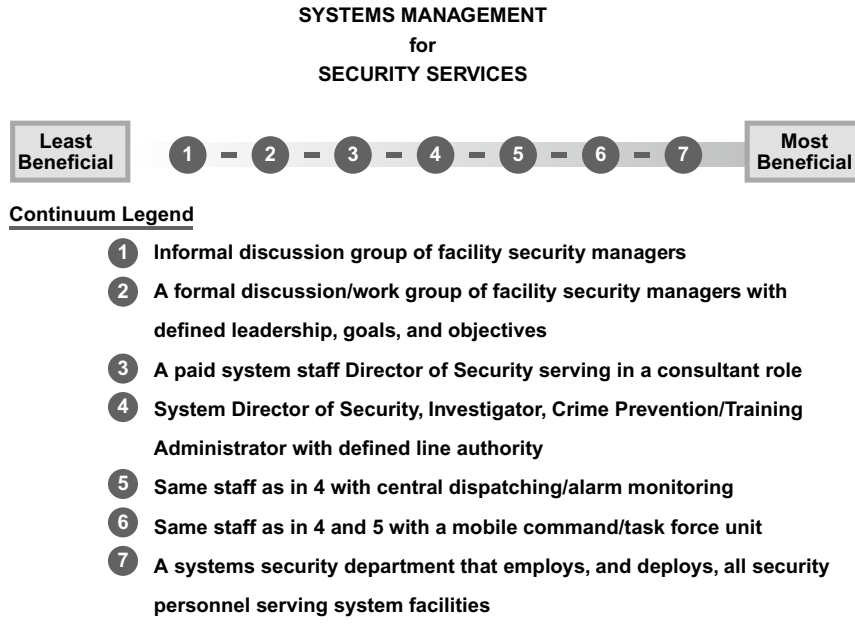
Figure 6-3 represents an example of a healthcare system corporate security organization chart, which incorporates a centralization of security support services while maintaining a certain management autonomy and program functions at the facility level.

There are numerous models that can be used to provide security services through a multifacility healthcare systems approach. Figure 6-4 portrays seven such approaches on a continuum from the least beneficial to the most beneficial.

## Types of Security Staff

Several options are available to healthcare administrators in selecting the type of security force to serve their facility. Each of the different models of staffing has its own advantages and disadvantages. The four basic types of security staffing are:

- Proprietary (in-house) staff;
- Outsourced staff (contract service);
- Proprietary security manager or supervisory staff with outsourced security officers;
- Off-duty law enforcement personnel.



**FIGURE 6-4** Comparing models in a corporate (multiple facility) security system.

There are also unique individual hybrid staffing models that utilize proprietary, outsourced, and off-duty law enforcement personnel in various combinations.

The security program is affected differently, depending on the general character/profile elements of the particular staffing model. [Figure 6-5](#) provides a summary comparison of the value of the different staffing models in relation to various security program components.

There is a significant trend toward the use of outsourcing as a model for security staffing of healthcare security programs. [Table 6-1](#) compares the security staffing models for a 10-year period. One reason that the proprietary model dropped so drastically, with a corresponding rise in the combination model, is that many healthcare organizations froze new hires but would allow vacancy replacements to be contract service employees.

It should be noted that the GE Security and IAHS HealthCare Benchmarking Study<sup>2</sup> reports that 77% of the 582 hospitals responding stated that their facilities utilized a proprietary security staffing model. This high percentage is in sharp contrast to the 34% as shown in [Table 6-1](#). There may be several reasons for this difference. The IAHS/GE survey report states that the survey returns were approximately 10% of the 7,461 surveys sent (381 returns completed the survey fully and 275 returns were partially completed), and that the returns skewed to larger hospitals versus the national population. It is a reasonable assumption that larger hospitals tend toward proprietary security programs and larger hospitals tend to respond to surveys in greater numbers.

	Security program components	Staffing Model			
		Proprietary	Outsource	Combination Out/Propr.	Off Duty
B U D G E T	Cost	Fair/Poor	Very Good	Good	Very Poor
	Cost Control	Good/Fair	Very Good	Good	Poor
	Cost Effectiveness	Good	Very Good	Good	Poor
O R G A N I Z A T I O N	Clear Chain of Command	Very Good	Good	Fair	Poor
	Organizational Control	Very Good	Very Good	Very Good	Fair
	Effective Training	Very Good	Good/Fair	Good	Poor
	Effective Supervision	Good	Good	Good/Fair	Very Poor
	Healthcare Expertise	Very Good	Fair	Good	Very Poor
	Effecting Program Change	Good	Good	Good	Poor
	Integration into Organization	Very Good	Fair	Good/Fair	Poor
	Loyalty to Organization	Very Good	Fair	Good	Poor
P R O G R A M	Lack of Turnover	Good	Fair/Poor	Fair	Fair
	Upward Mobility	Fair	Good	Fair	N/A
	Completing Good Documentation	Very Good	Fair	Good	Poor
	Quality of Investigation Activity	Very Good	Good	Very Good	Fair/Poor
	Crime Prevention Efforts	Very Good	Good/Fair	Good	Fair
M	Officer Image	Very Good	Good	Good	Fair/Poor
R A T I N G	Overall Effectiveness	Very Good	Good	Good	Poor

FIGURE 6-5 Comparing basic security staffing models.

Table 6-1 Comparing the Use of Healthcare Security Staffing Models over 10-Year Periods

Staffing Model	1980	1990	2000	2010
Outsourced/Contract	24%	30%	52%	55%
In-House/Proprietary	64%	60%	34%	31%
Combination of Proprietary and Contract Staff	8%	7%	13%	13%
Proprietary Management and Supervision with Contact Staff/Off-Duty Police	3%	2%	1%	1%
Off-Duty Law Enforcement	1%	1%	0*	0*

\*Less than 1%.

### Proprietary Staff (in House)

Proprietary staff simply means that the security department personnel are employees of the organization. The proprietary security officer may, or may not, be commissioned police officers. The vast majority, over 90%, of proprietary officers are not commissioned.

The proprietary commissioned officer is generally serving a HCF that is part of a university setting or a large hospital located in a state that allows certain organizations to maintain a fully commissioned private police agency.

The main advantage of the in-house staffing model is control. The organization can control the recruitment, selection, supervision, training, and compensation of security personnel. This degree of control is, however, adversely affected if security personnel are affiliated with a union.

The proprietary staffing system is generally the most expensive in terms of labor costs, despite the fact that some of the expenses are absorbed by other departments such as administration, accounting, purchasing, employee health, and human resources. Employee fringe benefits for an in-house staff generally range between 30% and 35% of the base salary of the employee. The utilization of a contingent of part-time staff will reduce fringe benefit costs; however, increased uniforms and equipment and training time will generally increase costs.

Some organizations ignore fringe benefits when computing program cost for periodic budget responsibility reports. The cost of fringe benefits can be controlled to some extent in larger forces by simply running a duty shift one or two employees short during holiday, vacation, or sick leave absences. This cost-saving method is usually not available in other staffing models. However, if the protection system can operate without a given position, the question of general overstaffing could certainly be an issue. The true hourly cost for proprietary staff can be significantly higher than for an outsourced staff. This higher cost is generally denounced by in-house budget staff that ignore certain cost items (such as overtime costs and other nonproductive payroll expenses) in order to achieve lower stated cost projections.

A main disadvantage of the proprietary system, in addition to its high cost, is the tendency for a program and its security staff to become stagnant. The routine of security services can easily produce lethargy among employees. It becomes increasingly difficult to stimulate and motivate officers in direct relation to their age and length of employment. The cliché “You cannot see the forest for the trees” becomes a real problem as a security officer becomes “one of the well-settled staff.” This does not imply that all in-house programs deteriorate to an unacceptable level. The implementation of good management techniques can successfully counter this negative trend. As a general rule proprietary security staff programs should not be considered for programs with a staff of less than 18–22 full-time employees. An in-house staff of less than this number of employees may also be mandated in the absence of qualified outsourcing service providers.

## Outsourcing (Contract Staff)

In addition to lower cost, organizations contract with an outside agency to be relieved of the burdensome administrative duties of operating an in-house security force. An additional incentive is that costs are fixed, and thus the organization can more accurately budget expenditures. According to *Security Magazine*, the use of contract security officers grows by 12% annually. About 10% of in-house programs in the United States convert to contract services each year. However, the net increase of contract services in healthcare

security is closer to 2%. There are some cases where a healthcare organization will convert to a proprietary staff from the contract supplied model.

Many other advantages of contracting for security services are espoused in articles usually written by members of contract agencies. Many of these arguments could be valid; however, too few contract companies live up to their claims in actual field performance. When one security company bids against another for business, the lowest bid most probably excludes something. Usually, what is missing is quality. A number of the world's largest contract agencies have formed a special healthcare services unit or hired a healthcare security practitioner to proclaim their expertise in healthcare security, a claim that should be examined closely.

The commonly propounded advantages and disadvantages of contract services, with countering or supporting comments, include the following:

1. *A contract service usually means lower payroll costs.* Unfortunately, lower cost security is almost always achieved by paying contract personnel a low wage and using a substantial number of part-time employees. The contract agency's full-time officers must generally work more than 40 hours per week to earn a sufficient salary. In some cases the wages are so low that overtime rates for contract security officers are lower than the straight-time wages of proprietary staffs. Excessively long working hours can be detrimental to the security effort, as coverage is not necessarily synonymous with good security. Having too many part-time employees, and a high labor turnover rate, can reduce the continuity of effort essential to a high-quality program. These deficiencies can be controlled to a large extent by including specifications in the contract agreement that specifies wages and benefits to be paid to the security staff.
2. *A contract service relieves the organization of administrative burdens.* This may sound like welcome relief for facility managers who do not want to concern themselves with managing the security function. The downside is that the facility can lose an important element of insight and control in achieving organization goals and objectives. Facility management must be involved with these so-called burdens, along with the contract service, to maintain an efficient and viable program. Facility management and contract security management must act as "business partners" to achieve an optimum protection system.
3. *Contract services can provide additional security officers as needed.* Employing extra officers on short notice or for a short duration of time may, however, require premium hourly payments. At best, additional security personnel who have never been trained at the facility may be of limited value. Further, when one client needs additional security officers due to a flood, civil disturbance, strike, etc., other clients may also need additional security coverage. All contract agencies have limits to the number of additional personnel they can provide and providing additional coverage may require an extended period of time before they are actually deployed on the client's property.
4. *Healthcare security personnel should be well versed in the specialized area of healthcare security services.* Contract agencies generally provide security services

to many different types of organizations and settings. Thus, it becomes virtually impossible for a viable contract security company to serve solely hospitals, airports, hotels, department stores, etc. There simply must be deployment of security personnel among the various types of accounts due to a variety of reasons including promotions, disciplinary problems, personality conflicts, officers' geographical residence in relation to the work site, and others. Even though a regular core of security officers may be assigned to a given account, it is common to temporarily assign a fill-in officer to cover for an unexpected absence. These fill-in officers are often nonproductive and their actions, or lack of action, may be contraindicated.

5. *Unproductive or undesirable contract officers can be handled by advising the contract agency that a particular officer is no longer acceptable for duty.* Contract agencies generally shift the officer to another client, who thus ends up with the first client's reject. Of course, it works two ways. An exceptionally good officer can be reassigned by the contractor to another facility without notice. The mobility and flexibility of such reassignments can create such a continuous change of personnel that continuity of service is jeopardized.
6. *Fraternization is a problem in all security forces.* Contract security officers are less apt to develop friendships that result in their overlooking problems that they should correct or report. They are often considered outsiders (this can be positive or negative), and with their high turnover rate, they have little time to develop close ties. Consequently, contract security officers can be more objective in discharging their duties. On the other hand, they do not always possess the same loyalty as regular employees and are not always as dependent on doing their best to ensure continued employment.

In competing for a contract security service, the lowest bidder usually provides only a warm body to fill a position. The low-bidder provided program is the most expensive system in terms of cost/benefit relationships. The cost of a security service should not be considered only in terms of labor cost, but also in terms of the total annual expenses and the quality of protection services provided. In many cases labor coverage can be reduced by using better-quality personnel, and annual costs can be maintained or even lowered despite a higher labor unit cost. A competent security consultant can be useful in analyzing security officer deployment schedules and objectively recommending the proper coverage plan.

A major deficiency in the contract security system can be traced to the client, not the contract agency. This deficiency is a lack of involvement in the day-to-day protection needs of their facility. Management cannot eliminate its role in the security of the facility by simply delegating the responsibility of protection to a third party. A third party, no matter how competent, cannot by itself provide the protection required. The organization that expects the contractor to take care of all of its security is not properly managing the organization's protection program. This *laissez faire* type of management practice, which can be viewed as the scapegoat syndrome, is characterized by organizational management that willfully



or through ignorance is not doing their job. If a serious crime, fire, or disaster occurs, management can simply point the finger at the third party as the one who failed to perform the job properly. Incompetent management often fosters the attitude that they can “correct the situation” by replacing the contractor. Obviously, the real problem is only perpetuated.

### Combination of Proprietary and Contract Security Officers

A staffing system of proprietary and contract security officers is a staffing methodology utilized in a number of facilities. The basic premise of this approach is a partial answer to the control and supervision problems that can occur when the facility staffs with all contract security personnel. Proponents of this combination system suggest that the in-house supervisor can develop a more in-depth program and make better use of security personnel. The in-house supervisor, an employee of the organization being served, presumably has direct lines of communication within the facility organizational structure. A very serious pitfall of this system can result from an employee of one organization acting in a supervisory capacity over the employee of another organization. In-house supervisors tend to be overly critical of the quality of the contract personnel furnished, and they are less motivated to work with the security officer in dealing with deficiencies than if the supervisors had made the hiring decision themselves. In-house management may tend to become less realistic and concerned in terms of line staff issues. This potential apathy can seriously affect the quality of day-to-day security operations.

### Off-Duty Law Enforcement Personnel

The employment of off-duty police personnel has lost favor for the vast majority of US HCFs. This system for securing a facility, even in part, is the least desirable of all staffing systems. High costs, virtually no organized system, little or no security-specific training, and lack of continuity are all basic reasons supporting this conclusion. Moreover, moonlighters of all types can be accused of just putting in their time as a second job provides supplementary income rather than being the primary means of support.

Police authority often has appeal to organizations that are not well versed in their protection needs. The power to arrest is often cited as a primary advantage of the law enforcement officer staffing. Most professional security administrators, however, view this authority as a disadvantage in terms of public relations and often promote outcomes out of proportion to the seriousness of a situation. Further, progressive police administrators prefer that their officers not work in off-duty jobs requiring them to wear the police uniform. The potential for misconduct, which brings adverse publicity to the police agency, and the possibility of the agency finding itself as a defendant in a legal action are situations to be avoided.

Although not in the healthcare setting, one case involved two Denver, CO, moonlighting (off-duty) police officers. This case, a shooting death by police, resulted in a civil trial against the city alleging unreasonable force depriving the victim of his constitutional rights against such force. Although no criminal charges were filed against the officers, the jury awarded the plaintiff \$500,000.<sup>3</sup>

Another disadvantage of using law enforcement officers is availability. A facility may have no coverage at a time of critical need because of overtime required on the officer's regular police assignments (strikes, fires, civil disturbance, training, etc.), court time, and federal assistance programs that fund police operations through the payment of overtime work. Police operations require the routine scheduling of police officers to meet changing conditions and emergency situations. Some of these emergency situations may be the same event(s) that directly affect the healthcare organization, requiring elevated manpower needs.

## Commissioned Police Officers

There are a few limited programs, such as the Baylor Health Care System, Dallas, TX, Cleveland Clinic, Cleveland, OH, and University of North Carolina Hospitals, Chapel Hill, NC, which operate a security program as a full police agency under the authority of state legislation. These types of programs are often referred to as Departments of Public Safety.

Another unique approach to providing security services via police officers is a law enforcement agency that has a security division. The security division is a contract agency available to private organizations. In this approach the organization contracts for police officers who are assigned to provide security/police services. The police officers are assigned to the organization as their primary work assignment as opposed to the off-duty approach. This type of program for HCFs is highly suspect in terms of value and appears to be a contraindicated approach for most healthcare organizations.

## Shared Services Approach

During the past 15 years the true shared service approach in providing security services has been somewhat changed and altered by healthcare organization mergers, affiliations, and the growth of proprietary hospital organizations. These new healthcare systems simply combine facilities through an organizational structure, as opposed to a shared service membership of separate individually governed facilities. The advantages and disadvantages of the shared approach to security must now be applied to a healthcare systems approach, rather than individual hospitals that had equal status in the governance of the shared services organization.

Although changed, the shared services security approach continues to flourish and is operating a significant number of highly successful hospital security programs. A major roadblock to the shared systems approach to security is that the separate organizations being served as a combined security system continues to be politics, turf, and self-interests.

There is another quasishared service approach operating to a limited degree. This approach is purchased services, or sold services, in which one healthcare organization markets a program to one or more other healthcare organizations. The organizational structure for this type of plan is relatively uncomplicated. A healthcare organization that has effective management and a specialized talent in security can generate additional revenue to offset costs while providing a quality, cost-effective service to other independent organizations. The provider organization must maintain acceptable services within a price structure, and the consumer organization has limited responsibility except when

extensive capital investments are required. In the case of capital investments, a long-term contract may be required to protect the provider organization. This approach is generally limited to, and is fostered, when organizations are in a very close geographical proximity to each other. This type of a shared security program has had little growth due to the often silent factor related to being a competitive organization.

### Corporate (Systems) Approach

The systems approach, like the shared service approach, is as much an organizational structure as it is a staffing model. Security services provided to facilities through the systems approach can produce a high level of service within an extremely cost-effective framework. Protection service lends itself particularly to a systems concept because one of the major problems in healthcare security is one referred to as “islandism.” Islandism simply means standing alone, attempting to protect oneself without the benefit of knowing what security-related situations are occurring in other local or systems HCFs.

Security problems that occur in one facility will very likely be transferred to other facilities in that geographical area. When thieves find out how easy it may be to steal computer equipment in one medical care facility, they are quick to “case” other like facilities. Forged prescriptions, short-change operators, and “professional patients” provide examples of problems that tend to travel the HCF circuit. Healthcare workers who are terminated due to involvement in security-type problems invariably turn up in other HCFs. Where else does a registered nurse find ready employment? Even housekeeping employees, food service workers, and maintenance people tend to seek employment in other HCFs once they have been employed in the healthcare field.

In a health system centralized approach, cost containment is achieved through several factors. One is supervision. A combined supervising effort can reduce the total number of supervisors from that required by individual programs.

Another area of cost containment is the purchasing of supplies and equipment—otherwise known as *economy of scale*. Supplies such as forms and uniforms are less expensive when standardized and purchased in large quantities.

Although important, cost reduction is not the primary reason to develop a centralized systems approach to security. The primary reason is to improve services. Improvement can occur in many areas, most notably in supervision, the training and quality of personnel, the investigative effort, and the efficient deployment of personnel, especially when the facilities are located within close proximity of each other.

Most facilities, except the very largest, may find it difficult to justify the high cost of hiring and retaining a top-quality security director or manager. On the other hand, several facilities within a system (each sharing only a part of the cost) can easily afford a competent security administrator and in turn reap the benefits of a quality protection program for their respective facilities.

The lack of direct supervision is a deficiency found in many healthcare security programs. Generally only the larger security programs can efficiently and effectively provide

24-hour supervision. In many facilities there may be only one or two security officers on duty on a given shift. It is not practical to staff a supervisor to provide supervision for one other officer. Some programs attempt to resolve this deficiency with a lead officer or senior officer when two are on duty at a time; however, this arrangement seldom provides true quality supervision outcomes. The systems supervisor concept is practical, efficient, and simple. When each facility is funding only a fraction of a wage, it is possible to pay a higher wage, thus attracting and retaining a better qualified supervisor. The number of personnel and the size of the geographical area that a supervisor can effectively cover are determined by individual philosophy, workload, level of officer training, and other factors.

Virtually every review of security operations, in healthcare and other settings, cites a deficiency in security officer training. There are probably few programs where the training level is at an optimum point; however, the systems approach provides a good opportunity to economically upgrade the training effort. The large group of personnel, the different facility environments available, and the sharing of cost enable a systems program to improve officer training. It is much more efficient to present a formal class to 8, 12, or more than to pay an instructor to present training for one, two, or three officers. The large personnel base allows the placement of officers in different assignments depending on their aptitude and skill level, giving the training effort an added dimension for the trainee and the operations supervisor.

Training takes on many different forms. One important form provided by the systems approach is the rotation of assignments. An important objective of training is to prevent or mitigate the problem of officers getting stuck in a routine. Rotating officers to other facilities within the system provides a unique training experience and fulfills the objective of having a pool of officers who have been trained in multiple facilities.

It could be argued that this advantage also exists for the contract agency, but there are some important differences. First, the contract agency must provide more general security training, since the officers may be working in completely different environments. Furthermore, it is extremely difficult for the contract agency to assemble officers for training due to their coverage commitments and generally large geographical service area.

A systems security program generally attracts a higher-quality applicant than either contract agencies or single facility in-house programs. The main attraction for candidates is the career ladder that larger organizations can offer to individuals who strive to move up to supervisory positions. The training and challenge provided through gaining experience in multiple facilities also contribute to attracting and retaining quality personnel.

Perhaps one of the most important and extremely cost-effective benefits of the systems arrangement is in investigation. Just as law enforcement problems move from city to city, security problems move from facility to facility. The consolidation of records and reports enables system participants to resolve incidents and problems that they would be unable to solve individually. In addition, the system organizations have an opportunity to preclude problem staff members from moving from one facility to another in the system. This is *preventive action* of the highest level, and preventive and mitigation action is the primary objective of any protection program.

Another benefit of the centralized investigative effort is the opportunity to foster better police/security relations by providing law enforcement agencies more direct access to organizational information. Law enforcement can develop a rapport with just one individual, or unit, rather than have to seek out the responsible security person in each facility. Likewise, if a law enforcement agency has information that would be helpful to all facilities in a given area, it is more likely to pass on this information to one contact than to contact a multitude of facilities.

The central reporting of incidents leads to another advantage, which is the exchange of information. Matters of common interest can be researched with results and/or conclusions distributed efficiently to the various facilities in the system, eliminating costly, time-consuming duplication of effort. The amount of time and money spent by each facility in sending a representative to security and safety meetings can be drastically reduced. A designated security representative from the system can represent all facilities. Information, ideas, and techniques can then be shared within the system.

The systems approach also allows basic facility security policies and procedures to be standardized to some degree. Standardized procedures such as package inspection, accident reporting, fire codes, incident reporting, and the like greatly benefit organizations as general staff and security staff transfer or rotate from facility to facility. A degree of standardization also facilitates more meaningful “benchmarking” when comparing certain data facility by facility.

The systems approach presents the opportunity to use more efficient security officer deployment patterns. Each facility has different and varied security requirements. The physical layout, the types of patients, the facility’s philosophy, and other factors create unique assignments. Likewise, each security officer is an individual and fulfills his or her responsibilities uniquely. Regardless of the applicant selection process, it is difficult to predict job performance until the officer is actually working. Given the larger base of operations, officers can more often be placed in a position that closely fits their job expectations as well as achieving performance that meets the expectations of the organization. System officers can move to another facility within the system without the organization losing the cost of their previous training. Preservice training will be required in the new facility; however, the required amount of training will be reduced to cover only specific facility requirements, as the officer is already trained in the systems general security program. Preservice training is further reduced in relation to the extent that the system has been able to standardize security forms, procedures, and policies.

The use of an officer who “floats” between two or three facilities is another important advantage of the systems approach. In some facility deployment plans, an additional security officer may be required on a temporary or intermittent basis, but not enough to justify a full-time officer. In these instances an officer may split his or her time among several facilities and thus be available for back-up and specific assignments for each—in other words, a shared security officer with costs shared according to the time deployed at each specific facility.

In short, the systems approach allows security administrators and planners many opportunities to use dollars, labor, and equipment in new and innovative patterns not possible in individual stand-alone facility programs.

## How Large a Staff Is Needed?

When a CEO or COO asks how much security staff is needed it generally means, “what is the least amount of security needed to get by?” The number and types of security personnel required for an efficient security program is a fundamental question for every facility. It is not as easy as applying a simple formula using the square feet of buildings, campus acreage size, number of beds, number of employees, comparisons to “like” facilities, or any other profile data. It is indeed an individual facility question since the numerous factors that must be considered vary in depth and scope from organization to organization. To arrive at the required number of security personnel, it is necessary first to analyze and understand the security mission, determine the level of the organization’s security risks and vulnerabilities to be managed, review physical safeguards in place, and identify the various services to be rendered. The next step is to design a program that will support the mission, properly manage risks, and implement the intended services. Only then can the number of staff required to operate the program be determined.

### IAHSS—HEALTHCARE BASIC GUIDELINE, #02.07

#### **Security Officer Staffing and Deployment**

**STATEMENT:** Several primary factors affecting the staffing model required to provide reasonable protection for the HCF and its patients, visitors, and staff. Staffing must provide for inspection, response, and service capabilities.

An HCF’s philosophy may emphasize a responsive (after-the-fact) posture or more strongly toward a preventative posture. Additional factors to be considered include but are not limited to crime analysis, HCF incident history, duties and expectations of the security department, physical and electronic security measures deployed, type and size of space to be protected, and other variables such as square feet, numbers of persons on site, and campus acreage to be protected.

#### **INTENT:**

- a. Staffing levels are best determined after conducting a security risk assessment by a competent security professional or security administrator (see Guideline 02.01).
- b. No single formula determines an appropriate staffing level for a given HCF. That said, a consideration of the factors listed below can lead to a reasonable and appropriate staffing configuration.
  1. Philosophy of the Organization—The level of protection provided and the services rendered by the security department are based on the individual facility’s philosophy and identified priorities to meet their unique needs.

2. Staffing Models—The most used staffing models include proprietary, contract, off-duty law enforcement, and various combinations of same. Smaller facilities, without dedicated security staff, will likely assign responsibility to other departments such as Facility Services. Regardless of the model selected, effective training must be provided.
3. Crime Analysis—Consider the type and volume of criminal activity occurring in and around the HCF. Also consider potential untoward circumstances in the event the HCF may provide services to crime victims (i.e., being a Level I Trauma Center).
4. Incident Activity—The severity and frequency of past on-site and nearby incidents will help determine staffing levels.
5. Emergency and Service Response Time—In cooperation with senior Administration, develop acceptable average security response times for both emergency response and routine service requests. Track, trend, and monitor these response times.
  - i. Priority I—Emergency situations such as crimes in progress, fire, and other emergency codes
  - ii. Priority II—Urgent calls such as patient assists and responding to incidents
  - iii. Priority III—Routine calls such as unlocking an office, patient valuables, motorist assists, unlocking or locking perimeter doors, etc.
  - iv. Priority IV—Scheduled tasks such as opening or closing gates, preventative patrols, opening conference rooms, wheelchair recovery, etc.
6. Patrol Frequency—Establish a desired frequency of routine day-to-day patrol. In planning patrol areas and frequency, it is helpful to divide areas up into the following general areas:
  - i. Security Sensitive Areas (see Security Sensitive Areas Guideline 09.01)
  - ii. Parking Areas
  - iii. In-Patient Bed Areas
  - iv. Clinic Areas
  - v. Public Areas
  - vi. Ancillary Patient Care Areas (Radiology, Labs, Physical Therapy)
  - vii. Support Areas such as Food Services, Medical Records, Maintenance and Engineering, and Administrative Space
  - viii. Satellite/Off-Site Facilities
7. Fixed Post Assignments—Unnecessary fixed post assignments may reduce the ability to provide for proactive patrol and effect response times if resources are limited.
8. Response Capabilities of Police and Fire Services—The availability and timing of law enforcement and fire responses may affect the staffing model. A lengthy or unpredictable response by outside agencies will usually require additional HCF-based staffing and capabilities.
9. Scheduled Routine Functions—Evaluate the number of scheduled functions such as cash escorts, pharmacy escorts, locking and unlocking areas, deliveries, equipment checks, or other similar duties separate and apart from routine patrol.
10. Scheduled Special Functions—Based on the crime analysis of the location and within the guidelines of the HCF, provide for crime prevention activities such as personal safety talks, security assessments, and security consultations designed as a proactive service of the security department.

11. **Nonscheduled Activities**—Evaluate nonscheduled activities that are routinely performed by security personnel such as investigative activities, problem resolution, lost and found, unscheduled locking or unlocking, patient assists including mental health watches (see Guideline 02.04 Security Role in Patient Management), processing court documents, acting as a witness, or preparing incident reports. It is not uncommon that these types of activities may take up to 50% or more of the individual officer's working time.
12. **Special Assignments**—Evaluate special events and celebrations which may dictate the use of significant staffing allocations.
13. **Fringe Benefits**—Examine fringe benefits including paid time away from work for vacation, sick time, etc. In certain models this may affect the staffing and deployment model, which may determine the need for overtime utilization or part-time or per diem personnel to maintain consistent staffing levels.
14. **Training Time**—A calculation of the amount of training required for the HCF is also helpful in determining number of hours required for staffing.
15. **Square Feet**—The total square footage/acreage of the HCF is but one factor related to security staffing and deployment and should not be used as an exclusive factor in determining staffing levels.
16. **Patient Volume**—Patient volume based upon time of day, day of week, or seasonal factors can have an impact on security staffing in the areas of fixed posts and scheduled and nonscheduled activities and must be considered.
17. **HCF General Staffing Levels**—Reductions in other HCF staff due to reduced patient days or other factors may result in the need for additional security personnel to provide increased patrols of unprotected areas.

**REFERENCES/GENERAL INFORMATION:**

- Colling, Russell L. *Hospital Security*. Fourth ed. Boston, MA: Butterworth-Heinemann, 2001, pages 121–144.

**Approved:** February 2009

## Staff and Line Positions

Staffing is generally viewed in two categories: staff positions (support) and line positions (field operations). The staff positions include training coordinator, investigator, crime prevention coordinator, security system specialist, and documentation/communications supervisor. The line positions for field operations are fixed post, patrol/response positions, and working shift supervisory personnel. Security systems monitors and/or dispatchers may be considered as either support or field operations personnel.

In some healthcare security programs the organizational structure includes a hybrid mix of staff and line positions. An example of this mix is to assign to a senior security officer, sometimes referred to as a Security Technician, additional responsibility for a functional segment of security operations. These additional functional areas of responsibility may include administrative and line activities for such areas as lost and found, key and lock



control, general staff orientation and training (i.e., new employee security presentation and operating department in service security training), new security officer training and orientation, and periodic physical security safeguard field inspections.

## Staffing Level Considerations

It may be helpful to view the calculation of the right amount of security staff for a given healthcare organization into categories. These categories are hard data goals/information; soft data analysis/projections; and subjective considerations/projections. [Figure 6-6](#) provides a summary of security staffing considerations.

### *Hard Data Goals/Information*

This category of staffing considerations is quantitative, and thus can be measured in terms of real number data sets and goals.

- *Emergency Response Time.* It is absolutely critical to excellence in patient care and the safety of staff and visitors that the healthcare organization provides the resources to effectively respond to critical incidents. These incidents may be

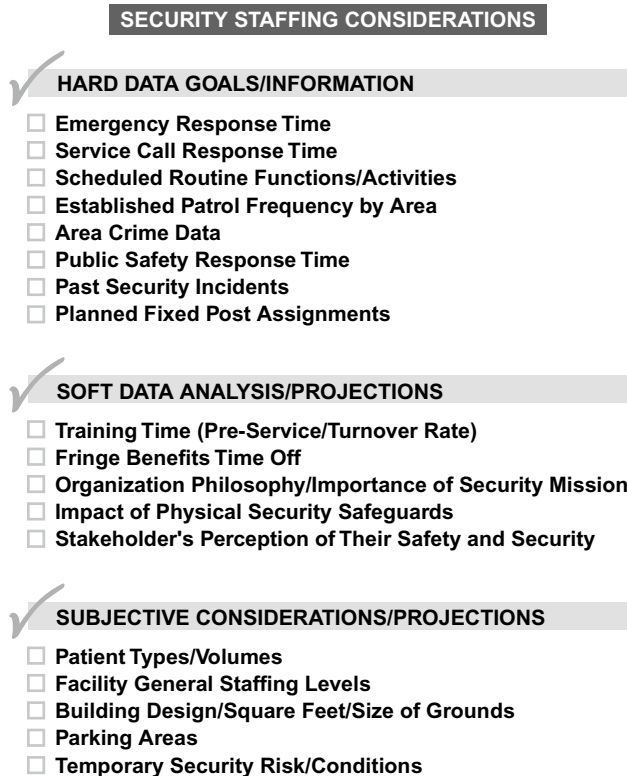


FIGURE 6-6 Summary of security staffing considerations.

criminal in nature, due to exposure to hazardous materials, weather related, or due to fires or accidents. Staff response time can be the major difference between life and death or other damage control. The HCF must maintain a capability to respond to critical incidents in a timely manner and such response should provide a competent skill level of action. The response time goal should be within three to five minutes of notification. Patient care areas, both inpatient and outpatient, should receive the shortest response time with support areas (i.e., warehousing, maintenance shops, and food preparation) only a minute or two later. When the Security Department is considered the first responder to critical security incidents it needs to be staffed and trained accordingly to meet the planned response time.

- *Service Call Response Time.* Service calls are sometimes referred to as *nonscheduled duties*. It has long been accepted that the security function includes the provision of all kinds of services requested by stakeholders. The security department's image, and often its ROI, is sometimes judged more on the services provided than on a preventive or emergency response capability. While response time is not generally critical in providing services, it is important in building stakeholder satisfaction and a positive security department image. The quicker a request for service is accomplished, the more favorable the security image.
- *Scheduled Routine Functions and Activities.* Operational planning for staff deployment often has the goal of limiting scheduled duties due to the flexibility that must be maintained to respond to the unexpected. Nevertheless, there will always be scheduled duties for security, such as cash escorts, lock ups, unlocks, and raising/lowering flags. These duties have a way of requiring time management somewhat out of proportion to the time it actually takes to perform the duty.
- *Established Patrol Frequency by Area.* When establishing security patrols there must be a defined expectation of the frequency of such patrols (inspectional services). Frequency in this regard does not mean an established time; rather, it means an expectation of how often an area will receive a patrol inspection. Frequency of patrol expectations is different for different areas, time of day, and day of the week. The security staffing requirement is dependent on a mathematical approach to developing time requirements in meeting frequency goals.
- *Area Crime Data.* An important element in determining the number of security officers needed to staff the department is the question—"How safe is the area from a crime perspective?" The answer to this question will impact the size of the security staff differently for different facilities. An inner city hospital that virtually has no external grounds and does not have numerous fragmented parking lots is basically factoring out the need for an extensive external patrol. Many such facilities that fit this profile have property lines that are sidewalk or street sides of their buildings. This situation does not mean the facility ignores or is not concerned with neighborhood crime—it simply means that the organization cannot take on the role of city policing. The security program itself will work with law enforcement agencies to develop strategies to create a safer neighborhood.

- *Public Safety Response Time.* The response time of the Public Safety agencies serving the facility will impact the security staffing level. Just as TJC requires hospitals to be “sustainable” for a given period of time when disaster strikes (emergency management), so must the facility be prepared to be “security sustainable” until help arrives. Small or medium size towns and municipalities may be able to provide four- or five-minute 911 response, while there are “horror” stories of half-hour and more of wait time for 911 calls in some of the world’s major cities.
- *Past Security Incidents.* It has been said that a predictor of future security incidents can be found in the review of past security incidents. It is hoped that this bit of advice is only partially true, as a properly managed security program will take corrective actions to avoid the repeat of a serious incident. It is true, however, that past incidents, especially recent serious incidents, serve as powerful motivation for the organization’s leadership to take a serious look at security staffing needs—security is too often incident-driven.
- *Planned Fixed Post Assignments.* The number of, and the location of, security fixed posts will influence the requirements for frequency of patrol and security emergency response times. A fixed post, especially an access control post, is providing several elements of security at basically the same time. Through proper access control screening procedures there may be an impact of a less frequent need of internal patrols. While controlling access the security officer’s presence is important in promoting a “we are protected” image in deterring negative actions. This presence is also beneficial in establishing the “feeling” of safety and security as perceived by the stakeholders.

### *Soft Data Analysis/Projections*

This category of staffing considerations is basically a combination of subjective and hard data, and is based on projected assumptions of security operations.

- *Training Time (Preservice/Turnover Rate).* The impact of training time relative to security staffing needs will vary from facility to facility. This variance is due in part to the type of security staff (i.e., proprietary and contract), size of staff, quality of officer training, and staff turnover rate. In organizations that utilize a contract staffing approach, the training time does not appreciably impact the number of deployed security officers, as the training time has been factored into the contract. In this respect, everyday post assignments (field deployment) are fixed and filling all posts is the responsibility of the contractor along with associated costs. Preservice training of new security staff members is also generally the responsibility (cost) of the contractor.
- A serious operational flaw in proprietary staffing systems is the ability to “run short” shifts—in other words, to fluctuate staffing of shifts depending on the number of officers reporting for a duty or to maintain a full staffing schedule through use of call-in part-time staff or the use of overtime. Since overtime money is not

unlimited, and generally not looked upon favorably by administration, too many programs follow the practice of “short staffing.” This practice results in reducing the level of facility security that in essence falls below the standard of care set by the organization. An opportune time for “Murphy’ Law” to come into play, short shifting can also occur when staff terminates. It is not uncommon that it takes six to eight weeks, or more, to fill a vacated officer position in the healthcare organization. The bureaucratic Human Resources of most healthcare organizations inhibit replacing terminated officer positions through various roadblocks. These roadblocks include not authorizing a replacement hire until the terminating employee is actually off the payroll and often well beyond this point; mandatory job posting within the organization; delay in recruitment processes; delay in applicant background checks; delay in the starting date. Unfortunately, this delayed process more often than not results in excessive overtime cost.

- *Fringe Benefits Time Off.* This consideration for calculating the number of security officers required is fairly easy to determine with defined vacation and sick-day benefits. As employees build longevity the amount of paid time off work increases. The unknown is the amount of time off work for such things as medical leave beyond paid sick leave, leaves of absence for a variety of reasons, including military service and family emergencies.
- *Organization Philosophy/Importance of Security Mission.* There are simply some healthcare organizations that give a high priority to patient, staff, and visitor safety, and there are those where safety is espoused but sufficient resources are not provided. It is difficult to determine whether this lack of “understanding the need” is due to lack of knowledge, lack of real concern, or extreme pressure to maintain an expected bottom line. Security is something that can be gambled with if an administrator is so inclined.
- *Impact of Physical and Electronic Security Safeguards.* It has been said that most physical security safeguards do not reduce security manpower requirements—they basically increase the effectiveness of the security officer. The truth of the matter is that certain physical security safeguards may increase the number of security personnel (not necessarily security officers) while other safeguards can reduce manpower loading. It is not only the safeguard but also the manner in which it is utilized. As an example, a CCTV system (or video surveillance) may be installed that is real-time monitored or the system simply records images with no live monitoring. On the other hand, a video surveillance system, along with audio and lock release capability, could be installed to control access points that were previously staffed by fixed post security officers. Another example is locking of a care unit, such as Pediatrics, that had no impact on number of staff, but simply increased the level of security of the unit. Each physical security safeguard must be examined to determine the amount of security staffing required to support the safeguard objectives.
- *Stakeholders Perception of Their Safety.* A major driver of security program development is how the staff perceives their personal safety and to a lesser degree

the perception of patients and visitors. Patients generally presume that they are safe and secure within the walls of the facility. Visitors are generally more concerned with their safety as they come and go, especially at odd hours. The visitor also has a general perception of safety in the specific neighborhood. There is nothing that is quite as assuring as the presence of a well-groomed, easily identified, competent and helpful security officer. Well-trimmed shrubbery, good night lighting, parking areas close to the facility, and well-controlled facility access enhance the perception of security and safety.

### *Subjective Considerations/Projections*

This category of staffing considerations is based on projections of patient profiles, general staffing levels, anticipated renovations or additional space allocation, and emergency reactions to the need for increased short-term security.

- *Patient Types/Volumes.* The types of patients and the number of such patients being treated (inpatients and outpatients) require a subjective conclusion regarding security staffing requirements. The facility with a level-one trauma center treating 75,000 to 80,000 patients a year, a large population of forensic patients, both open and secured mental health units, will naturally require more security than the small urban general medical/surgical treatment facility.
- The visitor mix is somewhat related to the patient mix. Trauma, mental health, and forensic patients tend to bring a different set of visitors than the small neighborhood treatment facility.
- *Facility General Staffing Levels.* Facility staff provide a primary element of facility security. Staff can observe persons in their work area and in general know who belongs and who should be queried concerning their presence. When general staffing is at a proper level, there are more eyes and ears “watching the store.” When staffing is substandard, these eyes and ears are not only reduced in number, but staff is stressed to meet minimum patient care standards. They are more narrowly focused on performing their primary tasks. When staffing is low, there tend to be more floats, per diem, and registry staff that by nature do not provide the element of security awareness or concern that regular staff provide.
- *Building Design/Square Feet/Size of Grounds.* Building design of main facility treatment and support areas is a major factor when calculating security staffing requirements. The size of the campus grounds and placement of separate buildings and parking areas are also important. What is of little significance is the number of occupied square footage—it is all in design. It is acknowledged that the higher the square footage of occupied space, there will generally be more patients, more staff, and a greater demand for security services. The security staffing impact of square footage in regard to these factors is calculated in the other various considerations, i.e., response times, patrol frequency, calls for service, and routine activities, which do to some degree relate to size.

- *Size of Facility.* Relating the size of the security force to square footage is somewhat akin to the long abandoned law enforcement approach to advocating the number of police officers required to population census numbers. Neither approach has any validity.
- *Parking Areas.* Parking areas have a tendency to heighten concerns of security and safety for most people. These concerns are intensified when parking areas are dark, devoid of other parkers, and remote from the ultimate destination. Parking areas can be protected to some degree through the use of appropriate physical security safeguards; however, the presence of a uniformed security officer is reassuring to most people. Providing this presence at the appropriate times can be labor-intensive, especially when there are a great number of small parking venues fragmented in various remote campus locations. The consideration of a high level of security officer presence in these parking areas will certainly test administrative leadership's philosophy of safety and budgeting support.
- *Temporary Security Risks/Conditions.* In all but the smallest of security departments, there will be constant requests (often demands) to provide "extra" security officer coverage for special situations. It is common for security administrators to shift coverage assignments almost on a daily basis. Some of this shifting is planned in advance (i.e., special events) and some shifting of officer deployment is at a moment's notice due to the development of increased security risk (i.e., patient assist/watch, threat of targeted violence, extended period of security incident scene protection, missing patient search, termination standby, community event, and fundraiser). It is generally not feasible or practical to schedule extra officer(s) for such needs; however, when officers are shifted from their normal deployment, there are certain security voids that are created. How large is this void and the organization risks incurred? It is a security management challenge that relates to establishing the level of security officers needed for the specific organization being served and protected.

In short, determining the right size security force takes a great deal of time, effort, and in-depth evaluation. Healthcare organizations commonly make the mistake of hiring a complement of security officers and then determining what activities they will perform. In a similar vein, some security planners answer every security problem by suggesting the hiring of additional personnel. More people are not always the answer, and in fact, numerous security programs have been upgraded by reducing personnel through improved management, specialized training, and the application of new preventive security concepts. Unfortunately sound planning and valid program justification often yield to emotions and easy solutions. In reality, more security personnel have been added to existing programs due to traumatic incidents than to sound planning.

### Staffing the Small Facility

The very small facility may not employ any specifically designated security personnel. In these cases required security activity is performed by maintenance, environmental

services, or other facility personnel. A small facility located in a relatively low crime area should provide, at a minimum, security officer patrol and called-for security response capability on a 24-hour basis if the facility has 75 or more inpatient beds, regardless of its location or perceived security risks.

Seldom does an organization suddenly decide to employ security personnel around the clock if it has never had an organized security system. As the facility grows, or faces increasing security issues, the facility will at some point in time face the need for security personnel. The first step in a security officer deployment plan generally involves coverage during the night hours. A coverage plan of 6:00 P.M. to 6:00 A.M. is a good first step. In organizations that are not required to pay overtime after 8 hours it is a consideration for an officer to work the entire 12-hour shift. This deployment plan allows for two officers to each work three and a half days each week, splitting the middle day, working 42 hours each week. The advantage of this deployment is that two officers cover the entire week, providing good continuity and consistency of program application. Some may argue that 12 hours is too long for one individual; however, it depends on the individual. In the case of this 84-hour-per-week schedule, one on-call or part-time officer would be required to cover scheduled or unscheduled time off of regular officers.

For the facility that currently provides night coverage, the next step in increasing personnel should be during the weekend. Although weekend days may on the surface seem peaceful enough, this is the time that general facility supervision is minimal, neighborhood street activity increases, and facilities are especially vulnerable to internal and external theft. The creative healthcare security administrator can find many nontraditional security duties that can be performed while still providing weekend day coverage.

All too often facilities attain night and weekend coverage and then have a tendency to stagnate. A 24-hour coverage increases the security posture of the organization two- or threefold. Instead of being forced to report property losses to security only during certain hours, for example, the organization can call on security officers at any time. When facilities assign another department or administrative person to pick up the security responsibility, when security officers are not on duty, the protection may fall well below an acceptable level of the standard of care.

When a program advances to providing one officer on duty around the clock, a program begins to take shape and becomes much more productive and effective. Security officer deployment during the day is geared to different activity than at night and on weekends. The day officer is usually the facility security supervisor. This officer takes part in committee meetings, works with various departments on planning and administration, and responds to calls for service. The day officer is the glue that solidifies all shifts of security into a unified program.

Facilities that provide 24-hour security officer coverage should consider one additional step: to provide 26-hour coverage. Under this plan there should be a 2-hour overlap of coverage during the primary night shift change period. One officer could remain on interior patrol while the second officer provides external coverage. It is recommended, however, that both officers be deployed externally. It is suggested that the arriving night

staff need security-preventive services more than the departing staff since the arriving staff are generally not grouped. Staff leaving at off hours must be provided the option of an escort service. Healthcare organizations now use many different staffing shifts, and traditional shift change times are becoming less distinct which may negate the validity of the 26-hour-per-day deployment plan for some facilities.

To staff an in-house program with 24-hour coverage for one position 7 days a week requires approximately five FTE employees. This number varies to some extent depending on the facility vacation, holiday, and sick time benefit. In the outsourced staffing model the required number of FTEs required is approximately 4.2 as the outsourced security provider is responsible for all nonproductive paid time.

Staffing problems occur when the schedule goes awry due to sickness, accident, no show, or termination. Untrained managers or supervisors often overlook this costly area of program administration during planning processes. Although this problem is rather straightforward, it is often not considered fully when an organization analyzes the financial implications of maintaining its own security force or contracting with an outside agency.

In programs that deploy one officer around the clock a staff of three full-time and three part-time officers works well. Part-time officers who are available to work additional hours to remedy planned or unplanned absences are valuable. Availability is an important criterion when selecting either full- or part-time employees.

## References

1. Dalton, D. (1998, June). Visions of leadership. *Security Management*, 29.
2. Weonik, R. (2008, January 21). *Securing our hospitals: GE security and IAHS healthcare benchmarking study*. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
3. Truax parents to get \$500,000. (1998, November 18). *Rocky Mountain News*, 4A.



# Security Force Administration

A common element of healthcare security programs is the utilization of physical security staff as a major component of the protection system. The development and preparation of the organization security force administrative plan are the basis for utilization of security staffing. The various elements or components of the plan must be addressed regardless of an in-house (proprietary) employment model or the use of outsourced personnel. A major task is selecting and retaining the best candidates to fill the security department's staffing complement and to implement sound management practices to achieve superior officer service. The three major operational components of the security force are thus *management, supervision, and security officers*.

## Management

The vice president, director, manager, or coordinator of the healthcare protection program is the single most important person in terms of determining program outcomes. This statement does not infer that the person charged with the responsibility to manage the program can do the job alone. There must be administrative support as well as buy-in from other organizational leaders, line supervisors, and obviously the security personnel themselves. The success of the security program, however, is largely the responsibility of the security management team and a direct reflection of their experience, leadership, responsiveness, and commitment to protection and customer service. If these qualities are not found at the top, they are likely absent in the security staff.

Historically, healthcare organizations have been rather vague in terms of defining the expectations and objectives of their security program. This systemic deficiency has in turn led to many organizations hiring ill-prepared persons as security administrators to lead this very important function inside the healthcare delivery system. A person who simply has a police or fire safety background or has experience with a state or federal law enforcement agency (regardless of specialty) may understand crime investigations, fire prevention, or other isolated elements of a sophisticated protection program. However, these individuals typically do not have the background in security or understanding of how protection principles apply to healthcare to properly manage a healthcare security program. Similarly, the security supervisor who has worked in the protection department

for many years, even as the number two person in charge, may not have sufficient leadership experience, skill level, or background to properly lead the staff.

Today, the security field is extremely competitive, and if one is aspiring to reach the top, it requires a high level of understanding of the industry, which can only materialize through experience and higher learning. Organizations today seek individuals who are academically prepared and who have relevant experience to direct their security programs. Relevant experience will, of course, vary depending on the organization's specialty or service.

Indeed, even the most experienced security administrators must continually seek further training, education, and self-development. There are at least six distinct activities that top-level security administrators must participate in as a professional:

1. *Review of the literature.* Healthcare security administrators must seek out pertinent healthcare security publications and electronic media as it becomes available. Although it is impossible to subscribe to every periodical or newsletter, buy every book, or attain all the information available, security administrators should do their best to keep up-to-date on current literature. Required reading should include material published by the International Association for Healthcare Security and Safety (IAHSS), Joint Commission Resources on the topic of security or emergency preparedness, or specific healthcare security-related councils of the American Society for Healthcare Engineering (ASHE)—Council on Safety, Security, and Emergency Preparedness—and ASIS International—Healthcare Security Council. These organizations have dedicated specific resources to advance the healthcare security profession and industry knowledge. They share their insights through various monthly publications, media, and formal presentations.

While most administrators maintain a personal library, healthcare and public libraries also are sources for this information. Tom Smith, CHPA, CPP, director of police and transportation at the University of North Carolina Hospitals and a past president of IAHSS, uses a simple, yet effective tool to stay abreast of current industry events and occurrences—free on-line alerts. Smith created several accounts with a major Internet search engine that provides daily e-mails with links to articles written world-wide with the words “hospital security” or “healthcare security.” Any words or combination of words can be chosen and used.

2. *Networking with peers.* The road of trial and error is often bumpy and no one should feel obligated to reinvent the wheel. Chances are that someone has the information you need or has faced a similar situation. Interactions with peers are also beneficial in detecting possible problems or circumstances that can lead to proactive programming. One healthcare security administrator makes prearranged visits to healthcare organizations when he is in another city on business—or even on pleasure—in order to meet another peer and see another security operation firsthand.

Membership in the IAHS is one of the most common platforms used for networking with peers. The Association provides discussion forums that allow members to get together and privately discuss issues or question of interest topic to them. This dialogue lets members share healthcare security industry-related information with their industry peers on a wide range of issues/topics. Many local chapters of IAHS, such as the Great Lakes Chapter in Michigan, use group lists that distribute e-mails to members in the region on specific security-sensitive topics, policy and procedure development, or elicit comments on new products, services, or ideas that help the healthcare security administrators improve the overall posture of security at their facility.

3. *Credentialing programs.* There are two primary credentialing programs for the professional security administrator. The first, and specific to healthcare, is the Certified Healthcare Protection Administrator (CHPA). The second is the Certified Protection Professional (CPP). These certification programs both require an extensive examination and a periodic recertification process.

#### *Certified Healthcare Protection Administrator*

Through IAHS, healthcare security leaders can achieve the highly coveted CHPA designation. Not only does this signify a high level of competence, it also demonstrates the individual's commitment to excellence and continuing study. The CHPA exam is administered by the Commission on Certification to individuals successfully qualifying for the exam. The program consists of progressive credentialing levels with qualified candidates accepted into the credentialing program at the Graduate level. Once this level is achieved each candidate has 18 months in which to become a CHPA. Each CHPA is required to recertify every 3 years by submitting documentation of continuing self-development, training, and education.

Once an individual has achieved the status of CHPA, he or she may become a fellow of the IAHS, and is designated as a CHPA-F. In order to become a fellow, the candidate must have completed a research project, resulting in a publication approved by the IAHS Commission on Certification. The exam is an oral defense of the paper by the candidate before a panel.

Although not a credentialing program, the IAHS Program of Distinction is the first level of the association's overall department accreditation program. Initiated in June 2006, the Program of Distinction recognizes healthcare security and safety departments within healthcare facilities that have achieved and maintained a minimum percentage of IAHS-certified security personnel.

Individual certification of officers and directors is granted to those who have successfully passed one of several certification examinations offered by IAHS. Certified personnel must maintain active certification either through renewal of their IAHS certifications at their current level or progress to the next level. Directors must maintain an active CHPA status through the IAHS.

## Certified Protection Professional

The CPP exam, administered by the Professional Certification Board of ASIS International, is not industry-specific. It consists of 200 multiple-choice questions covering tasks, knowledge, and skills in eight broad subjects identified by CPPs as the major areas involved in security management. The value of this credential is found in the documentation provided that shows the aspects, tasks, and knowledge that comprise a security professional's job. As with any course of study, the process of obtaining the CPP provides security industry exposure and the results of these studies ensure that the candidate understands the role of a security management professional.

4. *Seminars and educational programs.* The opportunity to attend healthcare-specific security and safety programs is limited only by time and funds. These programs are offered by the IAHSS, ASIS International, Joint Commission Resources, state and local healthcare organizations, ASHE, and a whole host of other trade associations and educational organizations. Healthcare security professionals should have little trouble finding such programs in their general geographical area or on a national or international level.

A minimum of one such seminar should be attended on an annual basis, and such attendance can generally be utilized as a credit in the recertification for CHPA and/or CPP.

5. *Contributing to the body of knowledge.* An essential element of self-development and keeping current is that of completing pertinent research. Research in this context simply means the searching out of information in the study of a specific aspect of security for either general information or data analysis to indicate a course of action.

This research may be of benefit to others in the field, and the true professional will seek opportunities to share this information with industry colleagues and students. The *Journal of Healthcare Protection Management* is but one of many trade publications that can be used as a platform to share. IAHSS, ASIS International, and other professional organizations also provide numerous opportunities to speak to industry peers about best practices and research conducted. As the old axiom goes “the teacher learns twice as much as the student.”

6. *Active membership participation.* Belonging to and being active in an organization such as IAHSS is a rich and fulfilling way to give back to the emerging field of healthcare security. Active membership is important to both the individual and leveraging the collective strength and influence of everyone involved in the healthcare protection industry—setting the standards for the future. By combining individual talents and skills with a diverse membership, innovative approaches to complex problems can often be achieved where an individual might feel at a complete loss.

Being a member of a professional security organization can be the platform or catalyst for reviewing literature, networking with peers, and contributing to the body of knowledge through information sharing.

## Selecting Management

Healthcare facilities have learned that spending the necessary time, energy, and resources upfront to develop a comprehensive security department mission statement to align the security program with the organizational expectations is well worth the effort. This process happens prior to recruiting or hiring the security administrator. The result is organizational clarity with the overall expectations of security and this demonstrates how important the protection program is regarded from the highest levels. It is essential that the design of the security program mirror and support the culture of the organization. Otherwise, organizational frustration in the protection program will, in all likelihood, be high.

It does not matter if the healthcare security management model is proprietary or outsourced; the leader selected to administer the security program must align with the leadership philosophy of the organization and be a fit culturally. If the organization follows the Plane-Tree model of customer service, senior leaders are going to want a building with an open and inviting atmosphere—they are not going to want a heavy “security feel” when patients and visitors first walk into the building. So if the security administrator comes with a bias for metal detectors and armed security officers, the likelihood of organizational fit will be very low.

### *Business/Technical Knowledge*

The healthcare security administrator must not only be technically competent and knowledgeable about security management and security systems but must also have a basic understanding of how to solve problems, set expectations, and hold people accountable. As a recognized leader in the healthcare organization, the security administrator should have a considerable understanding of the principles of finance/budgeting, human resources, and strategic management. In general, the healthcare security administrator must understand the healthcare organization’s mission, core values, and how it makes money.

### *Ethical Leadership*

Leadership is an obligation to the organization and employees to do what is right. Integrity and ethics are the most important attributes of leadership. Security leaders are the heart and soul of the protection department because they set the stage to create an environment and culture in which security supervisors and officers work and patients and visitors interact with security staff. Effective leaders help others to create the vision and understand the organization’s purpose. They provide the insight and the framework for making ethical decisions. By acting with integrity, leaders promote fairness and consistency. Leadership, therefore, is a “social” responsibility, a duty, and a trust—to manage the values of an organization.

When selecting security leadership positions, healthcare organizations must insist on the following values and ethical foundation:

1. Sense of integrity
2. Inspire trust and confidence in others

3. Lead by example rather than power, manipulation, or coercion
4. Respect for others.

A person who acts on his/her ethics is a person with integrity. Integrity means to do what is right, even when no one else is looking. The bottom line for life and business is ultimately people. “Business ethics” and “ethical/moral leadership” are inseparable components in the life of every healthcare organization. Ethical standards are basic to how patients, visitors, and employees are treated. Obstacles to ethical behavior and integrity are self-interest, self-protection, self-deception, and self-righteousness.

No healthcare security leader can do everything alone; they must learn to trust others—not just to succeed but for the organization to maintain continued existence. It takes courage to trust and empower employees with responsibility and entrust them with the authority to carry out that responsibility. Trust grows out of trust, and like respect, it must be earned.

Managing a healthcare protection program is not about personal identity, prestige, or status. Self-centered leadership will always end in failure. The impact of such leadership on an organization can be devastating. People become prisoners of the system and eventually focus on themselves to survive. The result for employees is a “me-first” attitude, self-interest before others, and unethical behavior. Control becomes imperative to the self-centered supervisor in order to maintain the status quo. Trust and teamwork are no longer possible. “Psychological beatings” will tear down self-esteem and group cohesion. Personal or organizational transformations are no longer an option. The loss of respect in leadership and growing negative feelings about the security department become the root for unethical behavior.

To get respect one must first give respect. It is fundamental to establishing, building, and managing relationships with others. Security professionals must be leaders with integrity and treat all people, regardless of their position or status, with dignity and respect, no matter what the situation. In short, the security leader’s job is to support the success of others. True leaders also know that the only persons worth hiring are the ones good enough to replace them.

## Supervision

The security supervisor is typically the person in the middle—a conduit who represents security administration to the security officers and represents the security officers to administration. The job of a first-line security supervisor has become increasingly complex. The supervisor is held to a higher standard of integrity, conduct, appearance, and performance than a nonsupervisor.

With the move away from the authority–obedience style of supervision, the application of many varied leadership factors must be applied.

To be a successful supervisor, one must acknowledge and put into practice basic leadership principles that include:

1. Setting a good example: Establishing the standard for attendance, attitude, and performance.

2. Knowing their employees and look out for their well-being: Caring develops cohesion and team spirit.
3. Keeping people informed: Using the communication tools at your disposal to keep people up-to-date on information pertinent to their jobs.
4. Developing a sense of responsibility in their subordinates: Delegating where appropriate, making sure the task is understood and are sure to follow up.
5. Training as a team: Helping all team members understand their roles without exception.
6. Making sound and timely decisions: Having courage to make objective and even unpopular decisions.
7. Seeking responsibility and taking responsibility for their actions: Using initiative to complete tasks without being told and taking credit for what they do: good and bad.
8. Being technically proficient: Fulfilling the role of a resource to their staff and understanding the resources available to them.
9. Knowing themselves and their limitations: Seeking to continuously improve their own abilities.

In short, they must accept ownership of their responsibility as a supervisor. A successful supervisor is characterized by being caring, committed, courageous, detail-oriented, disciplined, forthright, honest, interested, and professional. Thus, supervisory responsibility is not for everyone.

Much has been written about what makes a good supervisor. The quality of leadership is the one factor that stands out. Basic management traits are intertwined with the practices of effective leadership. Basic operational signs reveal how well a supervisor has developed the traits and practiced the principles. These signs are evident in the proficiency of the operation, the state of morale, and the discipline of the security personnel.

Successful supervisors analyze their strengths and limitations and work to strengthen the positive and never allow their limitations to become a liability. They resist the desire to be popular—a tendency that an officer promoted from the ranks must overcome. Supervisors must maintain a professional, business relationship getting results by developing trust, confidence, and respect in those they supervise.

According to Bonnie Michelman, CHPA, CPP, Director of Police and Security, Massachusetts General Hospital, “A supervisor must have a commitment to support the organization in all (their) actions and deeds. When the supervisor cannot do this, it is time to separate from the organization. This does not mean the supervisor will always agree with the directives and policies of the organization. And it does not mean that these directives and policies are always correct. Working for positive change is always a goal and responsibility of the supervisor. These efforts must be directed in a positive manner within the structure of the organization and not through ‘undermining,’ regardless of how noble and right the goal.”<sup>1</sup>

## Selecting Supervisors

Filling a supervisory position requires a decision of the highest magnitude. No matter how well planned a security program may be, its implementation is accomplished

by people. How well these people are supervised is a key to the effectiveness of the program.

There are two basic sources of supervisors: They may be recruited from outside the organization or promoted from within. Each source has certain advantages. The advantage of one can often be the disadvantage of the other.

Supervisors selected from outside the organization often assume their role with a high degree of objectivity. They have no preestablished friendships or animosities that must be negated, and they can bring valuable new ideas and techniques to the security operation. Moreover, they can be selected on the basis of demonstrated ability. They must, however, accept the fact that they must learn new organizational goals and objectives, as a first step in becoming a successful leader.

However, most organizations prefer to promote from within to create a career ladder. Promotion from within provides motivation and incentive for security officers who desire to advance in the organization. It provides an avenue and healthy perception that hard work, job knowledge, and good performance can result in promotion. The dead-end job has little appeal for the types of people who should be filling the ranks of healthcare security officers. Further, there is a direct relationship between turnover and correlation of job satisfaction with the availability for job promotion.

A problem often encountered is that relatively few front-line security personnel are qualified to be supervisors. It is a mistake to assume that a good security officer will be a good supervisor, because the tasks and functions of an officer and a supervisor simply are different. For this reason, a strong training and education program is essential to develop potential supervisors. Unfortunately, only a small percentage of healthcare protection programs are meeting this development need. The importance of such programs is further highlighted as the population continues to age and with it growing challenges associated with the scarcity of talent available to fill leadership positions and the growing propensity to change jobs in younger generations.

It is imperative that security administrators structure job promotion within a framework of objectivity. Position requirements and the method of selection must be established to ensure that personalities and prejudices are minimized to the fullest extent possible. The promotional structure should be fully understood by the rank and file to eliminate any possible misunderstandings and to allow officers to prepare themselves to participate in the selection process.

All officers possessing the prerequisites for promotion should be given the opportunity to communicate their interest, in writing, as the first step in the evaluation process. This process should be structured so the officer shares specific aspects of job knowledge and general understanding of leadership principles.

Afterwards, a common selection element is for internal candidates to participate in an oral interview. The candidates for this stage may be all those who submitted a letter of interest, or in the cases in which there are a large number of candidates, a certain qualifying approach may be required for continuing participation in the selection program. The interview may be conducted by a panel or the interviewers may meet with the candidates



on a one-to-one basis. If time and resources permit, the latter is preferred. The number of people to be included on the oral board is a matter of individual preference; however, the board must be limited to avoid overwhelming the candidate. As a general rule of thumb, no more than five people should interview a candidate at any one time.

Regardless of the system used, the interviewer should evaluate the candidates according to the traits required of the position. Before the interview, the interviewer should review a copy of the job description and the pertinent candidate background information.

Who should serve on the oral panel? In the healthcare setting, numerous resources are available. A mix of persons from different internal departments provides a comprehensive evaluation process. The composition of the interview group will vary from time to time, but it often includes someone from the human resources department, a clinical supervisor or manager (often from the Emergency Department), and a security supervisor or officer. In most cases, the security administrator renders the final decision regarding the candidate.

## Shift Supervision

The need to maintain desirable levels of staff performance is not unique to healthcare security organizations. The very nature of protecting a healing environment, however, does present some unique factors that shape supervisory activities. The quasimilitary structure of most security operations generally dictates a high degree of direct personal observation and interaction.

One of the major problems in supervising the work of field security personnel is the lack of clear and concise criteria for measuring the performance of everyday activities. In addition, factors such as time (24 hours per day) and area (large complexes) generally require a high proportion of supervisors to the number of line security personnel. In general, if there are three security staff members on duty during a given shift, one should be a supervisor. Not to be misconstrued as a recommended three to one ratio for supervisors to security officers, this practice suggests that a security supervisor should be on-site if there are three or more security staff members on-duty at any given time.

Supervision is the process by which problems and vulnerabilities are identified, solutions planned, and programs implemented. Shift supervision essentially consists of three broad tasks:

1. Communication: e.g., inspecting and documenting security incidents
2. Training and supervising employees
3. Monitoring of performance: e.g., conducting evaluations, enforcing rules and regulations

Only in the smallest of security organizations can all this be accomplished by one person.

## Communication

Few management activities are more important in dealing with personnel than effective communications, both upward and downward in the organizational hierarchy. It has been said that the essence of leadership is communication. George Jacobs, Former Associate Director of Security and Safety at Wake Forest University Baptist Medical Center, in North Carolina, has frequently been quoted saying “99% of all problems are a breakdown in communication.”

Hospital security officers must communicate with the people they serve each day, and there must be good communication between security officers and supervisors. Security officers, like most employees, want input into decisions that affect them. Supervisors must listen to employees; failure to be unresponsive to officer needs, or deliver deserved recognition, will result in team members disengaging and not performing to their capabilities.

The shift supervisor bridges the gap between the administrative staff, who develop and implement new plans or initiatives, and the field officers, who must carry them out. Thus shift supervisors spend a good deal of time being change agents. The supervisor must communicate program expectations and instruct and assist the field officer in its execution and evaluate the plan's effectiveness to provide administrative feedback. New directives involving field operations are invariably given to the supervisor for implementation.

Like most employees, security officers resist change “done to them” and accept change “made by them.” The resistance to change is a protective mechanism of employees who may perceive the change as a threat to habits, job security, or relationships. Resistance can take many forms, such as lack of cooperation, slowdowns, wild rumors, and individual or group behavior aimed at discrediting the change. Recognizing that change will meet some form of resistance allows supervisors to plan ways to communicate that will minimize this resistance. Perhaps the key element in this respect is to communicate the reason for the change, if possible. The rationalization for all directives cannot—and out of practicality need not—be explained to all individuals, including supervisors. Security officers and supervisors must maintain confidence in the management of the security system and accept day-to-day directives without expecting detailed explanations for each and every change.

## Training

Security officers must be prepared to subdue a mentally disturbed patient, apprehend a thief, comfort a distraught mother, escort a lost visitor, and perform any number of other tasks at any time, anywhere in the facility. The supervisor must help prepare security officers for this demanding job, properly training to make certain that the officer is capable of carrying out the task. Training develops confidence—priming the self-confidence in employees is one of the most fundamental responsibilities of a supervisor. Investing in the development of security staff creates a feeling that the organization, through the

supervisor, cares about their personal and professional success and in turn engages employee to perform at higher levels.

Training cannot be a one-time event. From the time they are hired and throughout their careers, security staff must continue training to learn, improve, and further develop their professional skills. This includes the supervisor being able to detect mistakes that may occur as the employees perform their responsibility. A system of controls must be available to prevent action that would seriously jeopardize the protection system if the subordinate is unable to carry out the task. In short, the supervisor must be able to verify the competency of his/her security staff in all required tasks.

The specific aspects of a comprehensive healthcare security training program will be further discussed in *Chapter 9, Training and Development*.

## Monitoring of Performance

The security supervisor not only has line authority over personnel but must also inspect their ability to perform the many functions and tasks of the position. The monitoring of performance typically requires three primary areas for the supervisor to examine: attendance, performance, and attitude.

### *Attendance*

A basic tenet for every security officer is the consistent ability to show up to work on time and when scheduled. The nature of most security officer schedules requires a strict adherence to punctuality that is unlike most traditional work environments. Failure can result in a lapse of required security coverage, exposing the healthcare organization to unnecessary risk for failure to provide adequate protection. If department policy requires security staff to remain on-site until properly relieved, the failure to do so can create inconvenience and dissention with fellow team members, not to mention the increased overtime expense usually undertaken when this occurs. A vital responsibility of a supervisor is to provide all the tools and resources necessary to support employees in their delivery of security service. Therefore, the supervisor must assure that everyone is at their position on time and ready to work.

### *Performance*

Supervisors should evaluate performance based on the sole premise of whether an employee can carry out the tasks required for the position. This evaluation requires finesse and may vary with the individual and is often situation-specific. In all instances, it requires direct observation of the employee's performance, appearance, customer service, etc. Many organizations use "line inspections" to carry out a portion of this obligation. Generally conducted by a supervisor, the line inspection is often oriented toward people and things (vehicles, equipment, and conditions) rather than functions. This type of inspection concentrates on the field officer's appearance, attitude, and deployment, and it includes on-the-scene observation of the officer's handling of an incident.

Many of the deficiencies encountered benefit by immediate, on-the-spot correction. Figure 7-1 shows a sample line inspection report.

Several techniques for monitoring performance do not involve direct observation or contact with subordinates. One of these techniques is the random interviewing of people

<b>SECURITY SUPERVISOR FIELD INSPECTION REPORT</b>		
Date:	Shift:	
Post:	Time:	Officer:
Officer Appearance:		
Post Conditions:		
Specific Element Inspected:		
Staff Contacted/Remarks:		
Corrective Actions/Remarks:		
Date:	Shift:	
Post:	Time:	Officer:
Officer Appearance:		
Post Conditions:		
Specific Element Inspected:		
Staff Contacted/Remarks:		
Corrective Actions/Remarks:		
Date:	Shift:	
Post:	Time:	Officer:
Officer Appearance:		
Post Conditions:		
Specific Element Inspected:		
Staff Contacted/Remarks:		
Corrective Actions/Remarks:		
End of Shift Summary:		
All posts covered: yes___ no__ explain:_____		
_____		
Calls for Service (#)_____ Incident Response (#)_____		
Total officer(s) shift time expended on: routine post activity___(hrs) incident response___(hrs) support services___(hrs)		
Use reverse side for additional post inspections.		

FIGURE 7-1 Sample line inspection report.

having contact with or served by the officer. These people—who may be complainants, victims, witnesses, administrators, or nursing supervisors—can be a source of information relative to the security officer’s attitude and how they handled a specific situation.

Another means of monitoring performance is the officer’s written report. The completeness and timeliness of reports are important evaluations of the officer’s performance in addition to how well organized or well written the report is.

Another useful technique is to conduct a review of an area that has been patrolled by an officer. An officer, of course, cannot be expected to observe everything, but much can be learned from supervisors who perform this type of inspection. A field inspection can help determine whether there are hazards or conditions that have not been corrected or reported by the patrol officer—it also benefits supervisors by helping them maintain knowledge of the specific physical area of the facility.

### *Attitude*

Monitoring the attitude of security staff is the most subjective factor when evaluating performance. Supervisors should look at specific instances of positive or negative behavior instead of a general feeling of good or bad. Supervisors should maintain a running history on each employee’s attitude that is maintained by chronological entry. This will help the supervisor and the employee remember the instances used to determine the evaluation. [Table 7-1](#) demonstrates a sample supervisor log of individual employee performance.

The morale of employees is a frequent topic of concern for top management, and often centers on negative attitudes. The supervisor plays a major role in maintaining the morale of subordinates. Obtaining desired performance cannot be accomplished solely by power, prestige, and authority. A supervisor’s real power is achieved through a network of satisfactory relationships with subordinates and upper management.

Negativity is contagious. A negative attitude of one officer can quickly spread and infect anyone exposed to it. But because an attitude is difficult to define and explain, we will focus on negative behavior. Negative behavior cannot be ignored, and the sooner a corrective strategy is undertaken, the better.

**Table 7-1** Sample Supervisor Log of Individual Officer Performance

#### **Supervisor Log**

Officer Smith received a positive comment for thoroughly checking the parking structures while on patrol on 1/3/09.

Officer Jones consistently had body odor and a wrinkled uniform when reporting for duty the week of 10/18/09.

Officer Greene spotted a trip hazard near the Main Entrance, marked it with a safety cone, and notified Facilities on 7/4/09.

I had to return Officer Browne’s reports because they contained many misspellings in the month of April 2009.

The beginning of a cure for negativity is professionalism and zero tolerance. The supervisor must be professional and demand professionalism from subordinates. Supervisors must keep negativity in mind and not allow it to become visible in actions or words. This is the first step. Next, the supervisor must have open and honest discussions with employees (in private) regarding perceived grievances or issues. Involvement by the employee in the solution agreed upon is important to the success of that solution. Sometimes there is no possible solution. In these cases, the supervisor must hold to the standards for employee attitudes and employees must understand what is expected of them and the consequences if they fail to perform.

## Relationship with Officers

Supervisors must maintain a professional business relationship with those they supervise. This does not mean that a supervisor is cold and impersonal. A supervisor can be friendly and open while still being a leader. It is important that a supervisor make sure security officers understand the relationship and then do nothing to violate the rules of the arrangement. Supervisors are expected to maintain a professional image and bearing at all times—setting the standard for appearance, attitude, and performance. It is up to the supervisor to make the most of the time spent with each officer and to give compliments or make corrections.

## Motivation

One of the basic responsibilities of supervisors is to instill self-confidence into their subordinates and motivate security officers to do their best. Motivation is very personal, and everyone will not respond to the same stimuli. Motivation also cannot be forced on an individual; thus the supervisor can only establish a climate in which employees can become motivated.

In general, staff want to do a good job and if they are provided the proper environment, they will do so. Motivating security staff requires that supervisors be aware of and practice certain basic principles. One of the greatest motivational acts a supervisor can perform is to listen to their staff—carefully and nonjudgmentally. Most people listen at about a 25% efficiency. In other words, we ignore, forget, distort, or misunderstand 75% of everything we hear. To improve, the supervisor must control external and internal distractions; providing a safe place for good communication to occur. The supervisor must be actively involved in the conversation, avoiding the tendency to interrupt. The supervisor who asks clarifying questions and checking understanding before the end of the conversation, summarizing what has been heard, and asking if that is what he/she meant will foster a culture of positive motivation.

Psychological studies indicate that recognition is one of the most significant factors in motivation, more important than responsibility, salary, advancement, or the work itself. A motivated staff do not need to be paid excessively, but do need to be paid excess attention. Subordinates must not feel that they are just another face lost in the group, but

rather that they are valued for their qualities as an individual. To motivate subordinates, supervisors must themselves be motivated and demonstrate a positive attitude. They must believe in the system and support all decisions handed down.

## Performance Management

All supervisors should understand that leadership perfection is not achievable—mistakes will occur when leading others. The very nature of a supervisor’s responsibility requires the supervisor to correct employees’ actions, provide specific direction in the midst of a security incident, or introduce a new policy and procedure. There are no leadership styles or rules and regulations that are universally accepted by all staff. The supervisor who manages with the hope to get consensus from all staff on all decisions will struggle with getting things done and, in the goal of trying to please everyone, will please no one. In either situation, staff complaints will arise in the course of duty, and the supervisor must be prepared to handle these situations.

The supervisor should start by putting his/her employee hat on. Look at what an employee wants from his/her supervisor/employer. It is quite simplistic. Employees want:

1. To **See** clear, understandable, and publicized rules or policies
2. To **Hear** performance expectations
3. To **Receive** frank feedback on performance and conduct
4. To **Be Treated** uniformly in the application of company standards and work rules
5. To **Receive** a thorough investigation of allegations of misconduct
6. To **Tell** their side of the story
7. To **Be Apprised** of the investigation outcome
8. To **Receive** warning before discharge
9. To **Use** a process of review by management other than their direct supervisor.<sup>2</sup>

## Performance Documentation

It is essential for supervisors and managers to document incidents of both greater and lesser significance, even if it is hard to see how the documentation might be used one day. When employees think of documentation, it is often associated with a negative feeling. Employees often recall a negative experience associated with some corrective action they have received in the past. However, performance documentation must be impartial. Simply put (from the perspective of an employer/employee relationship), performance documentation is a written account of an employee’s actions captured at a specific moment in time. Actions are measurable and quantifiable actions of a human being, and from a manager’s point of view. These actions may be favorable or unfavorable. However, it is important to come to an understanding that good performance documentation records behaviors that are actions.

**Table 7-2** Reasons for Supervisor Documentation

Reasons for Supervisor Documentation	
Create a History	Aid Memory
Identify Patterns or Changes in Behaviors	Encourage the Continuation of Positive Behavior
Cause Behavior Modification of Negative Behaviors	Add to the Credibility of the Manager's Version of Events
Prove an Employer's Case in a Trial, Arbitration, or Investigation	

There are many reasons for a supervisor to document an employee's actions. [Table 7-2](#) includes a list of many of the reasons why a supervisor should document an employee's actions.

Documentation is often important for reasons that no one could have foreseen. That is why it is essential for supervisors and managers to document incidents of both greater and lesser significance, even if it is hard to see how the documentation might be used one day. In a legal dispute, good documentation of the events leading up to or surrounding the discipline/discharge can be a crucial part of the employer's proof that the decision was proper and reasonable.

Good documentation is the employer's proof that the employer acted reasonably, that the employee was treated fairly, and that the employee was not disciplined and discharged for an illegal reason. The fact of the matter is that managers who do not, or cannot, properly document employee performance make themselves vulnerable to litigation, and increase their own difficulty in managing employee behavior in a fair way. For these reasons, and many more, the ability to properly document employee performance is essential to the success of any manager. So what actions should a manager document?

Supervisors must remember to document all actions, good and bad, great and small. Avoid ambiguous terms such as *insubordinate*, *attitude*, and *disrespectful* as they are vague. However, documenting actions in such a way that leads the reader to conclude an employee was insubordinate is invaluable. For example, writing, "S/O Jones was giving me an attitude" is not as effective as writing, "S/O Jones called me an 'idiot' while pointing his finger at me in front of patients and visitors in the ER waiting room."

Supervisors should document attendance, safety violations, violations of organizational policy, job performance, and on-the-job behaviors. Supervisors should not document gossip or rumors, off-duty activities, opinions or subjective impressions, personal characteristics, or hostile feelings toward a subordinate.

The overall purpose of good documentation and discipline is to bring about a change in behavior or an improvement in employee performance. The purpose is never to punish, humiliate, or otherwise embarrass the employee. Document your employee's positive actions and not just those behaviors you do not want to see repeated. Documenting positive actions is a surefire way to improve job performance, not only the actions of the specific employee, but also the actions of their peers as well.



So where and how should documentation be delivered? Positive documentation should be given in front of a group while performance documentation of a negative action should be conducted in private.

A manager's advantage when issuing corrective action is that he/she have the choice as to when, where, and what the circumstances of the environment will be. This allows a manager to plan out what he/she wishes to communicate to the employee, and under what conditions the communication will be delivered. When corrective action is given, the manager should have a clear and concise plan of how the interaction will proceed.

### *Documentation of Negative Behaviors*

Documentation of negative behaviors should contain facts, objectives, suggestions, and actions.

*Facts* are the who, what, when, and where of the situation that has occurred. Good performance documentation clearly states facts, and not opinions, and also differentiates between inferences and observable behaviors. Statements that include opinions or emotions are unacceptable.

*Objectives* are the written expectations or goals, and a reasonable timeline to meet those expectations or goals. Objectives should be measurable, attainable, and fair. For objectives to be fair they must be realistic. Unrealistic objectives lead to unmet expectations.

*Suggestions* are encouraged courses of action an employee can take to meet the objective successfully. Suggestions can include remedial training, the assistance of other employees, resource material or instruction manuals, progress meetings with supervisors, or solicited ideas from an employee. Remember that what is being measured is the objective, and it does not matter if the employee uses his/her own method to meet the objective, so long as the objective is met.

*Actions* are the communicated consequences the employee will receive if he/she fails to meet the objective(s). Action statements should be clear, concise, and fair. For instance, stating, "I do not want this to be an issue in the future," is not acceptable. Instead a statement such as, "If you take the facility keys home again, you will receive a written reprimand." The later example communicates to the employee clearly what will happen if the employee repeats the behavior.

### *Things Supervisors Should Consider Before Documenting*

Leaders and subordinates are first and foremost human beings. This can prove to be a problematic situation because all human beings make mistakes. This is why a leader cannot manage behavior in a vacuum separated from his/her subordinates' lives. An employee's life outside of work can impact his/her job performance.

In order to be fair, it is recommended that a supervisor should answer the following questions before giving an employee a corrective action.

1. What is the employee's record?
2. Has the employee had a fair chance to improve?

3. When was the employee first given a fair warning about the seriousness of the behavior?
4. What action was taken in similar cases?
5. What will the effect of your actions be on the group?
6. Are you going to handle the situation by yourself and when?
7. What other possible actions are there? Are there other solutions that can be used to bring about a change in behavior?

## Handling Problem Employees

The following checklist developed by Dr. Leslie M. Slote can help supervisors handle problem employees:<sup>3</sup>

1. What is the employee's past record? Always start any inquiry by assembling the facts to identify the problem. Has the employee committed this type of offense before? When? If punished now, should the employee receive a more severe penalty than a first offender?
2. Has the employee had a fair chance to improve? Review the employee's personnel record. Has the employee been given help in the past? Does the employee fully understand what is expected? Did he or she possess this understanding at the time of the offense?
3. When was the employee first given a fair warning of the seriousness of his or her behavior? Is there a record of this warning? If so, who gave the warning?
4. What action was taken in similar cases? Review similar incidents that have occurred in the department.
5. What will be the effect of disciplinary action on the group? Is disciplinary action fully justified? What will be its effect on others?
6. Are you going to handle this by yourself? Will you need to clear your action with someone else? Will you need assistance? What about the timing?
7. What other possible actions are there? What is in the best interest of the organization? The employee? Is another warning appropriate? Suspension? Termination?

## The Security Officer

The security officer is the point of contact for the majority of security services and activities. A clear understanding of officer authority is a baseline of operations. The recruitment, selection, diversity of staff, compensation, motivation, and officer discipline all interact to form an effective security force.

### Security Officer Authority

Most healthcare security officers operate with no more authority than the ordinary citizen. Defined by state statute, this authority is generally the right to prevent or stop the commission

of a criminal act in their presence. Security officers act as agents of the organization they have been engaged to protect, and thus their jurisdiction is derived from the organization. Jurisdiction, in this regard, is the legal power to exercise authority. The authority of officers to act on behalf of the organization should be clearly delineated in organizational policy.

What can happen when a security officer does not act properly? In addition to organizational discipline, the officer may be held criminally responsible or liable for civil actions. Criminal charges may include assault, negligent homicide, and battery. A wide variety of civil actions (torts) exists; malicious prosecution, defamation, false imprisonment, and slander are among commonly alleged actions. Not only is the individual officer subject to legal sanctions, but the employer might also be vulnerable. Employers may believe they are protected if the employee acts outside the scope of his employment. It should be noted, however, that the scope of employment may extend further than expected. The case of *Rivas versus Nationwide Personal Security Corp.*<sup>4</sup> is one example. A security officer became involved in an argument with a store manager and began choking the manager. Rivas, a store employee, witnessed the incident and screamed for help. The officer struck her in the face in an attempt to silence her. Rivas sued the security officer and his employer. The court held that the employer was liable and that the assault on Rivas was within the scope of employment because the incident arose out of an argument concerning the service the officer was performing.

There are, of course, valid defenses for the actions of security officers, but officers should bear in mind that they may be held to a higher standard for their actions than ordinary citizens. Citizens may be excused for their actions or inaction by reason of best intentions and lack of knowledge of a particular law, but security officers are expected to more fully understand the various provisions of the law. Security officers, by virtue of their training, experience, and responsibility, may be held to a higher legal standard than ordinary citizens. Thus security officers must understand their extent of authority and be well versed in the legal implications of this authority.

## Special Police Commission

In many jurisdictions, a special police commission may be conferred on healthcare security officers. These commissions are frequently used to help with street traffic control and ticketing and seldom provide additional authority beyond that of ordinary citizens.

On the other hand, commissions that give security personnel the same legal power as regular police officers carry an increased exposure to civil litigation. The actions of security officers with these special commissions are judged on the same level as those of regular police officers. The primary difference between special commissions granting full police authority to the security officer is that of time and location. These commissions often restrict police authority to the property of the employer and to the actual time the officer is scheduled for duty. Some very large medical complexes, frequently with a university affiliation, utilize security officers with full police authority. These departments are often referred to as Departments of Public Safety.

Security officers can generally perform more efficiently without police powers. The advantage lies in their ability to interview and otherwise interact with organizational employees and visitors within the scope of the employer–employee relationship. Security officers have much more latitude than law enforcement officers. For example, courts have consistently held that private security officers are not held to the provisions of the landmark Miranda case and need not advise the accused of their rights.

As a general rule, whenever a private citizen, including a private security officer, acts as an agent of the police, all constitutional limitations against the police apply. At times, police and security activities are quite similar, and joint activities raise certain concerns. It is sometimes difficult to determine when private security actions cease and public law enforcement takes over. Some lawsuits have been predicated on a conspiracy between police and security to violate the constitutional rights of others. Security officers should thus have a basic working knowledge of the Fourth, Fifth, Sixth, Eighth, and Fourteenth Amendments to the US Constitution and similar laws of other countries which concern the basic rights of the individual.

The exclusionary rule, which all states basically follow, is of particular interest to security officers. The exclusionary rule was intended to regulate illicit government conduct. In application, the rule excludes the introduction in a trial of evidence that a law enforcement agent has obtained illegally. On the other hand, when a private citizen seizes evidence, the evidence cannot be excluded from the trial no matter how illegal the seizure. Even though the evidence will not be thrown out of court, the citizen who seized the evidence illegally may not be free from criminal or civil actions. When security officers work in concert with a law enforcement agency, the exclusionary rule may well apply to any evidence seized.

## Licensing

Licensing for security personnel should not be confused with police powers. Licensing refers to the regulation and control of persons performing certain types of security services. A common aspect of many licensing statutes and some special police commissions is that of generating revenue (taxes) while doing little to regulate the delivery of protection services.

Most states have licensing laws, and many US cities have local statutes relative to security licensing. Many of these statutes appear to be directed at regulating the dress requirements of security personnel and the manner in which security vehicles are identified. These statutes, many drafted by law enforcement agencies, are intended to prevent confusion among the public regarding security personnel who look like law enforcement officers. This type of regulation is of course necessary; however, competent security administrators should make certain that security officers are not easily mistaken for police officers, regardless of the regulations.

Many licensing statutes border on the absurd and would probably not stand up under a test of constitutionality. One statute in a fairly large western city actually

prohibits the use of the word “officer” in “any advertising or upon the premises within the limits of the City...or on any of its vehicles or equipment.” The administration of some security licensing laws can pose great difficulty to sourcing and selecting quality security professionals. There is an acknowledged need for private security to be regulated with basic training standards established and criminal history searches conducted; however, those recruiting for security staff should be aware that many licensing requirements can add significant time to the hiring of new staff. The California Bureau of Security and Investigative Services (BSIS) requires a mandatory electronic fingerprint submission for all security applicants before granting a license to work as a private security officer. Mandated for both contract and proprietary security officers, the delay in obtaining the results of the criminal history check coupled with limited processing availability, makes it extremely difficult to hire new officers and to put someone new to the security industry to work. The delay can be up to 6 weeks or more based on the number of locations an applicant has lived in for the past years. As with the state of Arizona and a growing number of other states, the lack of a temporary license issuance program has severely limited the pool of available security applicants.

To upgrade and regulate the security function, good licensing laws are required. Professional security administrators can and should contribute to the creation of new statutes and ordinances that will eliminate the existing weak or misdirected laws, which are actually a detriment to safe environments. State licensing is to be commended and fostered, and municipal licensing should be actively discouraged. Meanwhile, there have been various attempts, through proposed legislation, to regulate security from the federal level of government.

## Selecting Security Personnel

The security force is often viewed as the quality linchpin in a healthcare facility’s security program. Often, security officers are among the first people patients and visitors see. They should create positive feelings about the facility and enhance the perception of safety within the organization. In short, the protection program needs a reliable and professional security team where the security employees are truly ambassadors for the organization and the customers they serve. In order to provide professional security officers, not just security guards, the healthcare protection program must have comprehensive, effective programs for recruiting, selecting, and retaining high-quality individuals.

Security work is not for everyone. Professional security managers review candidates from many different standards, but with one purpose in mind: to select an individual who is right for the job and to assign him or her to a position appropriate for their skill set. In order to obtain this cultural fit, it is necessary to hire employees who not only reduce the potential for an incident, but who also act responsibly when an incident occurs. Most security administrators agree that there are three primary skills needed to be successful as a security officer in the healthcare environment: excellent communication skills, aptitude to learn, and a customer service attitude.

Healthcare security work can be boring, routine, and monotonous, but within seconds can turn into a situation that challenges the mind and body to the limit. Perhaps no other position within the vast array found in the healthcare industry has such a wide expectation level. The expectations for a security officer differ widely among staff members and specific departments. Emergency department personnel want a security officer with great physical presence who can also de-escalate a verbally abusive patient. The night nursing supervisor wants someone who will diligently check and recheck the exterior doors. The psychiatric department wants someone who can be empathetic and apply sound psychological and social intelligence to control a situation. The risk manager wants someone with good investigative skills coupled with good report writing.

Employees also see security officers in many different roles, some of which are created by security officers themselves. One day a security administrator received a call from a night nursing service employee who complained that the new officer assigned to the parking lot was not doing his job and certainly did not compare with the previous officer. Upon investigation it was found that the source of dissatisfaction centered around frost on the vehicle windows. The previous officer had taken it on himself to scrape the windshields of departing staff but the new officer did not perform this service.

## Recruitment

There must be conscious effort to actively source security officer candidates. Viable applicants must be proactively recruited when a vacancy exists. Recruiting strategies must be continuously reviewed to ensure all appropriate sources are tapped for the caliber of person sought. In short, a security officer recruitment program should be planned and be an ongoing activity. Ideally, there should be between 7 and 10 applicants for each open position.

A very serious flaw of many in-house security departments is the time lag between the occurrence of a vacancy and the actual date the replacement officer is trained and ready for general duty. This delay is usually a result of the human resource department hiring process. This process can involve approvals required for replacement, posting of the position in-house, time delays in advertising schedules, preliminary screening, etc. This drawn-out process most often results in security shifts running short of staff and/or an excessive use of overtime.

Recruitment efforts will vary to some degree depending on the geographical unemployment rate. Various methods and activities can be used to attract security officer applicants:

1. *Employee referral program.* One of the most successful recruiting strategies is the word-of-mouth advertising generated from our employees that consistently provides most healthcare security programs with the highest quality personnel and staff. [Figure 7-2](#) is sample employee referral program advertising.
2. *Recruitment brochure.* This brochure is distributed in a variety of ways, from organized job fairs, school placement programs, retirement groups, to current



FIGURE 7-2 Sample employee referral program advertising.

officers who are encouraged to pass them on to others. One program reports that their recruitment brochure is handed out to all applicants regardless of the applicant being hired. Their philosophy is that even the rejected applicant may know of another person seeking employment who may be an acceptable candidate for employment.

3. *Signing bonus.* This recruiting incentive is also tied to a short-term retention objective. The basic concept is to pay a sum of money upon hire and then to pay an additional amount at some point of employment longevity. A 90-day period is common; however, many options are available within this concept.

4. *Staff recruitment monetary award.* This type of recruitment pays a current staff member a sum of money for referring an applicant who is subsequently employed. As with the signing bonus, there is generally at least one payment at a later time provided that the referred employee is still employed by the organization.
5. *Newspaper and newsletter advertising.* The newspaper advertisement remains the basic component for recruitment of healthcare security staff. Some organizations have also reported success by advertising in local business newsletters such as homeowners associations and church bulletins.
6. *Internet resources.* Monster, Craigslist, and other Internet postings can produce a consistent flow of candidates, reaching a diverse and computer-literate workforce.
7. *Open house and job fairs.* A well-advertised open house can attract a sizable number of applicants. This method of recruitment is more appropriate to larger organizations with multiple positions. Attracting too many applicants in a tight labor market can be counterproductive. Interested persons who are not hired or who do not get an interview are sometimes reluctant to return at a later time. This same problem may exist when utilizing a display booth at a job fair.
8. *Military.* Working closely with the military through transition programs, hiring events, and other advertising can consistently produce quality personnel who understand the importance of protecting critical infrastructures such as hospitals and healthcare organizations.
9. *Colleges and universities.* Proactively seeking out criminal justice/private security students provides a career path for these future leaders through internships, fast-track supervisory programs, and a “promote from within” philosophy.
10. *Law enforcement agencies and retirement organizations.* Security as a second career is commonplace in a workforce that commonly retires at an age where their maturity and experience can benefit the healthcare security industry.
11. *Senior market.* Mature adults who are looking to supplement their income can create a part-time contingent employment base for protection program.
12. *IAHSS.* Members and healthcare organizations can post their leadership positions and other security-based opportunities, providing a national and international recruitment exposure.

## Selection Criteria

Previous security experience is not of paramount importance in the overall selection process. In fact, the amount of retraining required is often a significant obstacle and cost. Even applicants with previous healthcare security experience generally need to learn new methods and procedures to function in the new system. On the other hand, applicants with previous security experience usually realize that duties, even in a good security system, are usually routine, requiring diligence and self-motivation. Another advantage is that the applicant generally understands that security is a 24-hour, 7-day-a-week operation. Applicants who have not been subjected to this around-the-clock schedule



often state that they are willing to work nights and weekends, but later discover that the new job does not fit their particular lifestyle.

Communication skills are an important factor in selection. The security officer must be able to communicate effectively in both oral and written forms. Written skills can be upgraded; however, improving oral communication skills requires considerably more time and money. The security department as a whole is often judged on the basis of security reports. Not all reports stay within the security section. The incident report, for example, is often used by the facility administrator, risk manager, insurance company, and law enforcement and other government agencies.

Image is another factor of extreme importance as it directly relates to the *presence* an officer will present. Many elements make up image, and a person either does or does not present a good image. Physical appearance and clothing are obvious items involved in applicant evaluation. Another characteristic of image often overlooked is the tendency to talk too much. Many times one is impressed with a person until he or she begins to speak. It is not always what is said, but how much is said. Security officers who present a good image have learned good listening skills.

Attitude, image, and pride all fit together and should be major considerations in any selection process. A positive attitude toward the job and the employer is a necessary first step in transforming a new officer into a seasoned security professional.

People are what healthcare is all about. Security officers must understand that their job entails a great deal of personal contact, and they must enjoy this aspect of the job or their performance will generally suffer. Good public and employee relations are an essential part of an efficient and effective security program. The one word that best describes a good security officer in the healthcare setting is *caring*. Officers must care about people, about their position, and about themselves.

Figure 7-3 demonstrates the basic traits and characteristics necessary for a security officer to be successful in the healthcare environment. No one candidate is going to flawlessly possess all of these skills; however, the security administrator or other hiring authority should develop an opinion about what skills are most important for the assignment.

Physical qualifications are controlled to some degree by government regulation. In the United States, federal legislation makes it unlawful for any person or agency to discriminate against any individual on the basis of race, color, religion, sex, national origin, or age. In some regions, this protection extends to sexual orientation. In setting physical standards, an employer must be able to prove that certain physical qualifications are required for the job. In a landmark Ohio case a court ruled on such aspects as physical strength and fitness, physical agility, height and arm's reach, ability to drive a car, and ability to impress others with psychological advantage of height. In each instance the court ruled against the defendants. It was unable to find rational support for the height and weight requirements. Although this litigation involved police officers, the implications concerning the hiring of security officers are apparent.

<p><b>Assertiveness</b> – A security officer must be direct and persuasive when dealing with others, have the ability to exert influence or direct a self-desired outcome</p>
<p><b>Empathy</b> – In general, an officer demonstrating empathy will be open-minded and flexible and should have the ability to identify, understand, and relate to the needs and reactions of otherpeople.</p>
<p><b>Confidence</b> – Successful security officers should have the capability to rebound from negative feedback or criticism and have the ability to approach and respond to situations in a self-assured and consistent manner.</p>
<p><b>Sociability</b> – The activities and tasks of a healthcare security officer provides ample opportunity to interact with other people. Security staff should be friendly, outgoing, and possesses the ability to initiate contact with others.</p>
<p><b>Helpfulness</b> – Accommodating, service minded, and team spirited, the healthcare security officer should be internally motivated to help others and work as part of a team.</p>
<p><b>Thoroughness</b> – Conscientious, with careful attention to detail, to protect a healing environment requires those individuals who take a personal sense of responsibility for the quality of their work.</p>
<p><b>Problem Solving</b> – Dealing with problems and issues that are complex and unique is a frequent requirement of the security officer. They need to understand and possess the ability to resolve routine problems.</p>

**FIGURE 7-3** Characteristics and traits of a successful security officer.

There are an increasing number of female security officers being added to the ranks of healthcare security forces. Not only have security administrators realized that women can do the job, but they also recognize that women contribute an additional dimension to the protection effort. Specifically, there have been a number of studies finding women, on average, can often more effectively de-escalate aggressive behavior than their male counterparts. Because the security effort in the typical healthcare setting must deal with many emotions and manage aggressive behavior, it stands to reason that female officer's should be welcome on staff. Female security staff can be used effectively in surveillance, checking women-only areas, searching female prisoners, transporting women in vehicles, and other such functions that may be sensitive for the male officer.

Just as with gender diversity, cultural diversity is an important aspect of a well-rounded security staff. A medical care facility with a population of significant ethnic cultures requires a security staff mix that represents these cultures. Security staff members who are available to speak different languages and interpret basic customs of different ethnic groups can offer great assistance in the mission of the healthcare organization. In general, the security staff should be balanced and reflective of the community served.

Managers often hire the best-qualified person, but if the candidate is overqualified, job satisfaction can suffer and with it individual and security department performance. Careful consideration should be given to offering employment to individuals who do not have a career commitment to protection or the healthcare industry.

## The Selection Process

In order to ensure excellence in security services, it is necessary to hire security officers who not only reduce the potential for an incident, but who also act responsibly when an incident occurs. To this end, every healthcare security program must develop a rigorous employee selection process that on a minimum requires compliance with the following basic requirements:

1. Have, at minimum, a high school diploma or GED
2. Possess excellent communication skills
3. Can read, write legibly, and speak English fluently
4. Have a customer service attitude
5. Have an aptitude to learn
6. Pass an employment background check, criminal history record check, five-panel (marijuana, cocaine, amphetamines, opiates, PCP) drug screen, and security threat assessment
7. Meet all local and state licensing requirements for security personnel
8. Have no secondary employment that could be construed as a conflict of interest with the facility

It takes a great deal of experience to effectively interview security candidates, and even the best interviewers are often misled by applicants. The application is the basic selection document and is used extensively in conducting the interview. During the interview process, the interviewer must find out as much about the candidate, within legal limitations, as possible in a relatively short time.

In many cases the interview is simply an effort toward gaining as much knowledge about the applicant as possible. Thus the interviewer should ask specific performance questions that can be used to predict future behavior and assess the motivational fit of the candidate in effort to identify the best applicant.

A common screening tool is the requirement for healthcare protection applicants to read a predetermined security incident scenario and write an incident report based on the facts provided. Much information is uncovered in this process, to include the

applicant's ability to read and interpret the English language as well as demonstrate their writing and critical thinking skills.

Because a group of applicants rarely yields the one individual who possesses all the qualities required for the ideal security officer, especially in a time of low unemployment, the selection process often results in comparing one candidate against another.

The most important part of the selection process is the background investigation of the applicant. The first step is to verify as much information as possible concerning what the applicant has written on the application form and has stated during the interview. Is the applicant the person they purports to be? Are there any conflicts of interest that exist? Is the applicant engaged in secondary employment with any enterprise doing business at the facility?

The most common and economical approach is through letters of confirmation, telephone calls, and personal contact. The best single predictor of what a person will do is what he or she has done. A criminal history record check, social security number verification, sex offender registry validation, and drug testing are each important aspects of the hiring process. A more detailed process of applicant checking is contained in another section of this text.

Federal legislation in 1988 prohibited most private employers from requiring polygraph examinations of employees or prospective candidates. Some companies have replaced the polygraph test with psychological exam/integrity tests and now use these to screen applicants. Used to assess varying degrees of aggression, impulse control, suspiciousness, over-controlled anger, and other psychopathology, there is considerable controversy surrounding the value and the possible negative impact of these types of screening tools. Most studies fail to produce any clear results on the credibility of these tests.<sup>5</sup>

The passage of the Americans with Disabilities Act of 1990 (ADA) has affected the security officer hiring process. In simple terms, an employer may not exclude hiring a person with a disability when it is not related to job requirements and the employer can make reasonable accommodations to fit the disabled individual into the work environment. As with most legislation, the law is rather straightforward; however, regulatory interpretations can be rather inconsistent.

The ADA requirements do not ban the use of psychological tests for pre-employment screening. The tests, however, cannot be constructed to screen out individuals with disabilities unless the disability is shown to be job-related for the position and is consistent with business necessity. A distinction is made between personality traits and mental disorders. It is generally accepted that employers may seek out broad personality traits in the pre-employment process as long as the process does not disclose a mental or psychological disorder. An examination performed after a conditional offer of employment has been made is the proper avenue to determine any mental impairment of the applicant. In fact, a medical examination is often a statutory requirement for licensing security personnel. The definitive resource on what constitutes a mental or psychological disorder is the *Diagnostic and Statistical Manual of Mental Disorders* (DSM) published by the American Psychiatric Association.<sup>6</sup>

Security staff must be in good physical health and condition, capable of performing normal or emergency duties requiring moderate to arduous physical exertion. Recently, many healthcare organizations have introduced human performance evaluation's (HPE) to test the physical capability of a security officer to perform the required functions of the position. Conducted only after a conditional offer of employment has been made, introducing this level of testing can help measure physical fitness and reduce costly worker's compensation expense due pre-existing injuries or the inability to perform basic functions and tasks required of the healthcare security officer. The essential requirement is that the physical requirements of the position must directly tie into the security officer position description. [Table 7-3](#) provides sample HPE measurements.

## Full-Time Versus Part-Time Security Officers

A security system cannot be effectively or efficiently operated with an overabundance of part-time security officers, nor can the program be operated with only full-time personnel. The appropriate number of part-time personnel depends on several factors. A highly structured system, with strong supervision and training, can successfully operate with a higher percentage of part-time personnel than can a program operating on an informal basis. It is a generally accepted rule of thumb that a healthcare security staff consists of no more than 20–25% part-time officers. An exception to this guideline would be officers who are regularly scheduled to work 32 hours per week. In some cases, an officer working 32 hours per week would be classified as a full-time employee.

A workforce consisting of only part-time officers cannot provide the continuity required of successful systems. Moreover, keeping the security staff informed requires constant attention, and full-time employees can generally be kept better informed

**Table 7-3** Sample Human Performance Evaluation Measurements

Task	Required
CARRY	Security Officer must transfer fire extinguisher from wall cabinet to area of need. Must be able to:
Distance 150'	Carry 25 lbs. for 150 feet, hold 25 lbs. for 30 seconds
LIFT/CARRY	Security Officer must transfer with assistance patient from floor to bed.
Vertical Ht. 2"–36"	100 lbs., 1 X in 5 minutes
PUSH/PULL	Security Officer must drag combative patient when trying to restrain the same 85 lbs., 1 X in 5 minutes
WALK 1	Security Officer must complete assigned foot patrols; must access all areas of hospital grounds, both inside and out, must respond to calls Walk 300 yards with twists and turns 1 X in under 3 minutes

through greater frequency of system interaction. Officers who work 40–48 hours per week are generally better informed than officers who work 10–16 hours per week.

Ironically, although part-time officers often possess higher qualifications in terms of experience and education, they are generally less productive. This situation can in large part be traced to the fact that part-time employees usually do not depend on the part-time job for their main source of income. This does not imply that part-timers are consciously not doing their best, but they often lack availability for training and flexibility in scheduling. The part-timer must generally schedule training and working hours around another job or other interests. One can only work so many hours in a day or a week without sacrifice to individual performance.

Part-time officers do fulfill an important need in most security departments, however, and should be viewed as a management tool. Just as overtime is an effective management tool, the part-time officer, when correctly used, can fill a void, especially in terms of cost containment. An important aspect of the part-time officer is flexibility. The ultimate goal is to employ part-time officers who are not only competent, but who can readily extend the number of hours they can work in the week. Even better is the part-timer who can switch days or shifts on short notice.

The result of using only full-time personnel is almost always that of overstaffing. Rarely does the right staffing plan turn out to be divisible by 40 hours, or in other words, an even number of FTEs. Thus an extra officer is often on a shift to provide the officer with a 40-hour week. Work always can be found for the officer, but it serves only to rationalize the schedule. Further, a staff of only full-time officers offers the department supervisor little choice but to operate short staffed or to use excessive amounts of overtime to fill shifts for vacations, holidays, sickness, and other absences. As a rule of thumb, the average number of absences for each proprietary employee is 33 days per year, or 264 hours. Subtracting 264 hours from 2,080 hours (FTE) leaves 1,816 hours of productive service. Utilizing this formula, it would require 4.7 FTE staff to deploy a schedule of one officer on duty around the clock 7 days per week, not including training time. Staffing schedules become even more complicated as much of the projected 264 hours of non-productive time is not predictable in terms of when it will be utilized.

A large suburban hospital in southeastern Wisconsin, faced with cost containment pressures, misguidedly used all part-time security officers in their department staffing and deployment plan in an effort to reduce their costs. Operating under the belief that if the department did not have to pay health, dental, retirement, and other hospital-rich benefits to the security staff, they could meet the administrative mandate to cut 10% out of the department's operating costs without reducing the number of weekly hours of security coverage. The organization quickly found that the increased training costs and uniform expense associated with the increase in staff substantially reduced the assumed savings. Employee morale tanked, patient satisfaction scores plummeted, and the overall perception of safety on campus fell, causing the hospital to turn over valuable healthcare professionals. All combined, the hospital actually increased their overall operating costs

and had to enter into a service recovery mode to improve the level of confidence the hospital had with the previous security department staffing model.

Thus, a proper balance of full- and part-time employees must be achieved. A program that requires one officer on duty 24 hours a day can be staffed with three full-time officers and three part-time officers. This system gives each part-timer 16 hours per week and provides a resource to cover additional hours as required. It is generally not productive to hire a part-time officer for less than 16 hours per week. It is also poor practice to employ only part-time staff on the weekends. As discussed, compared to the full-time officer, the part-timer may be less trained, motivated, and informed. Proper deployment of part-time staff is to intersperse their schedule with full-time officers.

## Wage Compensation

Determination of an equitable wage and salary structure is one of the most important phases of the relationship with security officers. For good employee relations, each security officer should:

1. Receive sufficient wages to sustain himself and his dependents
2. Feel satisfied with a relationship between his wages and wages of other people performing the same type of work in a like organization.

The wage compensation received by security personnel is often determined by a complex method of evaluating the nature of the job, the present worth of security services to the organization, and the effectiveness with which the officer performs the job. Working within the organization's wage and salary program, the basic rationale is to compensate fairly all employees in relation to their contribution to the organization's objectives. In a simple example, if the security officer contributed the same value as a radiological technician, the two wage rates would be the same.

One factor that affects compensation from a nonevaluation aspect is supply and demand. The healthcare organization may have to pay more for certain positions simply because there is a shortage of trained personnel to perform a particular function. In the structured system, the need to pay a higher wage than the evaluated worth is often referred to as a *red-lined position*.

Wage surveys in a common geographical area are often helpful in establishing the average compensation paid for protection services. Because cost of living differences and supply and demand produce wide salary fluctuations, comparing the wage rates of different geographical areas yields little valid information. In reviewing wage rates, one must be constantly aware that security functions differ with organizations, and job titles alone can mean very little when making direct comparisons.

A growing trend in healthcare security is to structure salary scales to training levels. This concept has been fostered in part by the progressive certification standards of the IAHS.

## Retention

Recruiting and hiring good security officers is not enough in an industry notorious for high employee turnover. The key is to retain staff. The successful healthcare security program works to reduce their turnover rates by implementing programs that support open communication and feedback, concern for the individual, competitive compensation, performance rewards and recognition, career advancement, and a positive work environment.

Keeping good security officers and supervisors is a high-priority objective of management. The cost of recruiting, selecting, processing, and training new security officers is significant. Estimates range as low as \$1,400 to as high as \$25,000.

Retention of security staff begins by creating a culture of continuous learning and offering career advancement opportunities. The challenge of protecting the healthcare environment is a great retention motivator. When coupled with a customer service orientation, the ability to collaborate with coworkers and feel a part of the team, being provided the resources to get the job done, and a sincere interest from senior management in their job, the protection program can overcome the plaguing issue of turnover that has negatively affected so many programs. Of course, a competitive base pay and overall satisfaction with benefits needed in day-to-day life must lie at the foundation for retention efforts to be realized.

However, retaining the wrong people can be counterproductive. A principle deficiency found in one healthcare security department program review was too little turnover. In this department of 14 officers, the average longevity was 17 years, with the newest officer being hired 6 years prior to the review. Complacency and negativity had settled in to the department. Security administrators must focus on developing a healthy turnover rate to keep a motivated and engaged workforce.

## Performance Expectations

Maintaining a strong degree of discipline is a high priority for security administrators who operate successful protection programs. Corrective action must be exercised to develop a security force amiable to direction and control. Security officers must set an example for the entire organization. Security officers are often deployed at the point of entry for patients and visitors and thus create a lasting impression. The organization must insist that security officers follow rigid regulations to maintain an impeccable image. Some security departments have shown such a professional approach by developing a code of ethics for security personnel or adopting the IAHS Code of Ethics identified in [Figure 7-4](#).

A security force with poor discipline exhibits the following general characteristics:

1. Low morale
2. Lack of direction, objectives, and goals
3. Inattention to duties



## IAHSS Code of Ethics

---

### Preamble

"Recognizing that the overall quality of healthcare delivery is directly related to the professional services rendered by the International Association for Healthcare Security & Safety, the following Code of Ethics is hereby mandated as a consideration for membership."

As a healthcare security professional, I pledge to dedicate myself to providing a safe and secure environment to the people and institution(s) I serve by:

- Supporting patient care and awareness within my healthcare facility
- Recognizing that my principal responsibilities are security and/or safety services to the healthcare community I serve:
  - to protect life and property and reduce crime through the implementation of recognized crime prevention and investigative techniques, and
  - to provide a safe environment of care in support of the mission of the healthcare facility
- Respecting the moral and constitutional rights of all persons while performing my duties without prejudice,
- Ensuring that confidential and privileged information is protected at all times,
- Maintaining open communication with other professionals with whom I conduct business,
- Striving to further my education, both academically and technically, while encouraging professional development and/or advancement of other security/safety personnel,
- Promoting and exemplifying the highest standards of integrity to those whom I serve while dedicating myself to my chosen profession.

**FIGURE 7-4** IAHSS Code of Ethics.

4. Careless attitude toward the job, supervisors, and organization
5. Common disregard for rules and regulations

Affecting a high degree of discipline in the security force begins by establishing clear standards and expectations for officer performance and behavior. It establishes a foundation for communication, hiring, training, promotion, and decision making and serves as the basis for accountability in the department. Its power is found that once a department has clarity in its mission and goals, it creates unity in all that needs to be achieved.

Holding security staff members accountable helps create department discipline. The security administrator must remember that security staff are people and people do what is inspected, not what is expected. Having high expectations is good but they must be about outcomes to be achieved and not prescriptive "how to" lists. So the security administrator or supervisor should ask themselves four simple questions when defining expectations:

1. Have you clearly communicated your expectations?
2. Do all team members fully understand their roles and responsibilities?
3. Are there current organizational environment conditions that hinder their performance?
4. Are there clear consequences for performance?

The consequences can be both positive and negative depending on performance. The positive consequences prompt the individual to do the right thing while the negative consequences restrain the individual from doing the wrong thing. Thus, disciplinary action, when taken, is intended to correct a deficiency and should not necessarily be regarded as a punishment. Regrettably, most disciplinary action is negative in nature; however, both positive and negative practices are valuable in the development of a security officer.

Figure 7-5 illustrates a method of recording positive and negative data, attendance, and general information concerning a specific officer. This record is intended to be a work history summary and is a useful tool in evaluating the performance of an officer. It can also serve as a primary document in any unemployment cases or violation of equal opportunity cases that may arise.

### Positive Reinforcement

Employee recognition programs are a particularly effective way to hold security officers accountable for delivering exceptional security service—and reward them for achieving it. Many organizations have introduced employee recognition programs to acknowledge and reward employees for many contributions made to the department and the health-care organization as a whole. Whereas most disciplinary action is designed to prevent a reoccurrence of a behavior or action, effective security programs will place significant

SECURITY DEPARTMENT				
SERVICE PERFORMANCE RECORD				
NAME:		POSITION:		
Date	Entry Description	Absent	Late	Source
04/01/09	Completed 90-day evaluation with satisfactory performance ratings			Lt. James
05/22/09		EU		Sgt. York
07/28/09	Remedial training on panic alarm response			
09/17/09	Officer commended for outstanding customer service by patient (see letter of appreciation in file)			Lt. James
11/08/09			L	Sgt. York
12/07/09		PTO		
12/24/09	Officer counseled on uniform appearance re: wearing white socks			Sgt. York
01/01/10	Officer awarded 1 year anniversary pin			Lt. James

Legend      Absent

Late

- Paid Time Off (PTO)
- Excused Unpaid (EU)
- Called Unexcused (CU)
- No Call/No Show (NS)
- More than 15 minutes (M)
- Less than 15 minutes (L)

FIGURE 7-5 Example security officer chronological history.

effort to acknowledge positive contributions. This encouragement sends a subtle but powerful reminder for the employee to repeat the behavior.

No formal reward and recognition systems can take the place of personalized recognition. If recognition is not personalized it can be demotivating and hurt individual performance. Paying attention to performance and celebrating success together reinforces department values and builds a powerful spirit of cooperation and teamwork.

## Rules and Regulations

Rules and regulations concerning the conduct of security personnel must be in written form so that officers are apprised of the ground rules that apply. Unwritten policy is not an equitable method of operating a security program. The guidelines identified in [Figure 7-6](#) are fundamental healthcare security principles that apply for all hospitals and healthcare organizations regardless of size, geographic location, or operating philosophy.

The following prohibitions are generally included in most policies, along with prohibitions peculiar to specific organizations:

1. Security officers will not become involved in discussions of religion or politics while on duty or on the premises of the organization.
2. Security officers will not engage in lengthy social conversations with other employees. This is extremely important for the proper functioning of the organization and the security department.
3. Security officers will not criticize any employee or regulation except to the proper supervisor.
4. Security officers will abide by the organization's smoking policy and will not smoke on exterior patrol.
5. Except during break time, there will be no eating and no reading of material other than material applicable to the job unless it is specifically authorized by a security supervisor.
6. No radios or TV will be allowed on any post.
7. Security officers will not leave a security assignment until properly relieved.
8. The loaning or borrowing of money among employees is prohibited.
9. No member of the security department will solicit contributions for any purpose, except by permission of the security department head.
10. Security officers will not write notes or letters to employees or visitors concerning security problems, nor will they write personal notes to such persons.
11. Security officers will maintain strict confidentiality of information relative to all persons and organizations obtained during the performance of their duty.

The last item on the list is such an important issue that it is not uncommon for organizations to have each person in the security department sign a confidentiality statement as a condition of employment. [Figure 7-7](#) is an example of such a statement.

## Fundamental Healthcare Security Principles

### BE PROFESSIONAL

CONDUCT YOURSELF IN A MANNER WHICH REFLECTS POSITIVELY ON YOU AND THE ORGANIZATION YOU REPRESENT

### MAINTAIN CONFIDENTIALITY

DON'T OPEN YOURSELF UP TO PROBLEMS BY DISCUSSING CONFIDENTIAL PATIENT OR SECURITY INFORMATION

### DO YOUR PART

DOUBLING UP AND OVER-SOCIALIZATION TAKES YOU AWAY FROM BEING AN IMPORTANT PART OF THE SECURITY TEAM

### SET THE EXAMPLE

DRINK, EAT, AND SMOKE IN DESIGNATED AREAS ONLY; FOLLOW ALL HOSPITAL RULES & REGULATIONS THAT YOU ENFORCE

### KEEP THE TEAM INFORMED

NOTIFY YOUR SECURITY SUPERVISOR REGARDING ALL MAJOR INCIDENTS; USE PASS-ON LOG TO ADVISE FELLOW OFFICERS ON SECURITY ISSUES

### BE DECISIVE

DISPLAY CONFIDENCE BUT KNOW WHEN TO USE THE CHAIN OF COMMAND

### COMMUNICATE

SUBMIT ALL REPORTS BEFORE THE END OF THE SHIFT TO ENHANCE ACCURACY AND THE FLOW OF INFORMATION

### PRESENT A POSITIVE IMAGE

FIRST AND LAST IMPRESSIONS ARE OFTEN THE MOST IMPORTANT AND LASTING ONES

### BE TRUSTWORTHY

EQUIPMENT AND SUPPLIES ARE FOR BUSINESS USE ONLY

### FOLLOW DIRECTION

WHEN PATIENTS ARE INVOLVED PROCEED UNDER THE DIRECTION OF A MEDICAL CARE PROVIDER

### LOOK SHARP

WEAR AND MAINTAIN YOUR UNIFORM AND EQUIPMENT PROPERLY

### BE RESPONSIBLE

REPORT FOR DUTY ON TIME AND BE READY TO WORK; REMAIN IN YOUR ASSIGNED AREA UNTIL PROPERLY RELIEVED

### STAY SAFE

THE PURSUIT OF PATIENT OR SUSPECT BEYOND SET LIMITS IS DANGEROUS AND DISCOURAGED

### LOOK TO ASSIST

CUSTOMER RELATIONS THROUGH SERVICE IS THE MOST IMPORTANT FUNCTION YOU CAN PROVIDE

### PROTECT YOURSELF

WHEN NECESSARY, WEAR THE PERSONAL PROTECTIVE EQUIPMENT AVAILABLE

FIGURE 7-6 Fundamental security principles.

### CONFIDENTIALITY AGREEMENT

I understand that in the course of my employment, I may have access to and become acquainted with information of a confidential, proprietary or secret nature which is or may be either applicable or related to the present or future business of the company, its research and development, or the business of its customers. It is my responsibility to in no way reveal or divulge any such information unless it is necessary to do so in the performance of my duties. Access to confidential information should be on a "need to-know" basis and must be authorized by my supervisor.

I agree that I will not disclose any of the above mentioned trade secrets, directly, or indirectly or use them in anyway, whether during the term of my employment or at any time thereafter except as required in the course of my employment with the company.

\_\_\_\_\_  
Applicant's Signature

\_\_\_\_\_  
Date

**FIGURE 7-7** Sample confidentiality statement.

## Disciplinary Action

In addition to general prohibitions, a listing of offenses for which the security officer may also be disciplined should be prepared. These offenses normally include the following:

1. Absence without proper notification.
2. Accepting any gift or bribe in the line of duty.
3. Conduct unbecoming a security officer or prejudicial to discipline of the security department either on or off duty.
4. Consuming alcohol or illegal drugs, being under their influence on duty, or reporting for duty in an impaired condition.
5. Bringing contraband to the workplace.
6. Enabling any person to secure stolen property.
7. False reporting.
8. Ignorance of rules and regulations after being duly informed.
9. Sleeping on duty or neglect of duty.
10. Excessive force or the improper display or use of a weapon.
11. Unnecessary harshness, violence, or profane language.
12. Willful disobedience of orders of a superior.
13. Failure to report any security incident either observed by the officer or brought to his or her attention by another person.

Written disciplinary policy should delineate the specific type of action that may be taken against an officer and the specific supervisors who may take that action. For example, the policy might include the following degrees of disciplinary action, all of which become part of the officer's personnel record:

1. *Employee counseling.* This action may be imposed by any security supervisor and is not normally considered a formal reprimand. However, it is intended to make the

officer aware of performance or behavior that, unless corrected, can lead to future disciplinary action.

2. *Verbal warning.* With a verbal warning, the supervisor discusses the problem with the employee and the employee is advised what must be done to correct the problem. The verbal warning is typically documented on a disciplinary action form; a signature received acknowledging the conversation and stored in the employee's personnel record.
3. *Written warning.* This action is more serious than a verbal warning or is a recurrence of a violation. It is a generally accepted practice that the written warning outlines the problem, the required corrective action, a timeline for improvement, and the consequences if the employee fails to correct the problem. The security officer's signature indicates he or she is aware of the contents of the warning but does not imply that he or she is in agreement with the reprimand. This form of disciplinary action may be taken by any departmental supervisor.
4. *Probation status.* This action lasts for a specific period of time, but typically does not exceed 60 days, during which the officer is evaluated to determine fitness for retention of employment. An officer on probation should not be eligible for overtime assignment, and the officer's merit review date advanced by the length of the probationary period. Probation status may be imposed only by the department head.
5. *Suspension with or without pay.* This action lasts for a specific period of time, not to exceed 5 working days. It may be imposed only by the department head and should include a follow-up meeting with the employee prior to returning to duty. An officer may also be suspended for a period of time by the department head, pending a review of alleged misconduct.

Note that an officer may be suspended for the remainder of the shift for any infraction of departmental rules and regulations, when in the evaluation of any security supervisor the continued duty of the officer may be prejudicial to the best interests of the organization. This suspension from duty should not be confused with the disciplinary action of suspension as a form of punishment.

6. *Dismissal.* Employees do not always improve their behaviors or performance following disciplinary action. Additionally, employees may do something so severe that the only appropriate administrative response is to terminate them. This action may be imposed only by the department head or higher authority.

## References

1. Michelman, B. (2004). Supervisor responsibilities. In: *Supervisor training manual for healthcare security personnel* (2nd ed.). International Association for Healthcare Security and Safety, Chicago.
2. York, T. W. (2007). Civil liability and the supervisor. In: *Supervisor training manual for healthcare security personnel* (3rd ed.). International Association for Healthcare Security and Safety, Chicago.

3. Costello, J. K., & Leibfried, C. (2004). Employee relations and employee appraisals. In: *Supervisor training manual for healthcare security personnel* (2nd ed.). International Association for Healthcare Security and Safety, Chicago.
4. The Spain Report: *Rivas v. Nationwide Personal Security Corporation*. 559 So. 2d 668 (Fla. App. 3 Dist. 1990), 1991, G1–21.
5. Office of Technology Assessment Staff. (1991). Summary of findings: Use of integrity tests for pre-employment screening. *Security Journal*, 2(1), 44.
6. Arnold, D. W., & Thieman, A. J. (1994, January). Psychological test in ADA's wake. *Security Management*, 44.

# Security Attire and Equipment

The attire worn by healthcare security staff and equipment carried by the security officer establishes the image of the protection program and, very often, the perception of personal safety for those who work on campus or visit the healthcare facility. The assigned responsibilities of and type of attire worn by security officers determines how the security officer will be equipped.

## Uniforms

There is a wide variety of attire options available to the healthcare security program. A continuous debate is whether security officers should wear a traditional uniform or a blazer and slacks. The security polo style shirt and matching uniform pants have recently entered the exchange. The consensus of healthcare security administrators is that security officers should not be outfitted in plainclothes.

The true plainclothes approach, identifying security only by the facility name badge, is practically nonexistent in the healthcare field today. Management, training, or investigative staff may wear business attire due to the nature of their individual role and function. However, not to equip security officers with a uniform, regardless of the style chosen, creates a mixed message about the importance of security to the healthcare organization. The lack of visibility and loss in customer service are unacceptable.

## Determining Uniform Style

The determination of which style of uniform should be worn by security staff strongly correlates to two specific categories: (1) organizational philosophy and (2) the primary function of the security staff. The healthcare security administrator must be sensitive to each when making a selection of which uniform should be worn by the security staff.

### *Organizational Philosophy*

The type of healthcare organization, its customer service philosophy, and administrative preference are often the primary drivers of what attire is worn by the security staff. For example, will the healthcare organization take its cultural cue from the Disney Institute? After investing significant capital expenditure to renovate the hospital lobby to make it a



welcoming and comfortable setting for patients and their families, seldom will the organization want a stern security feel when patients and visitors first walk into the building. In these instances, the perception of the security officer uniform by patients and visitors will be an important criterion in determining which style is worn.

Administrative preference may also take precedence over the style of uniform worn. Several years ago, a hospital administrator in a high-crime area in a downtown metropolitan hospital directed the security staff to move from a traditional military style uniform to the softer, blazer style uniform. When asked about the need for the change, the rationale was based solely on individual preference and previous experience. The administrator had come from a healthcare organization where the security staff wore the blazer style uniform and he preferred it. Neither the negative perception of personal safety expressed by hospital staff nor the advice of healthcare security experts deterred the decision. Fortunately, the administrator was transferred to a different position before the change could be carried out. Although this was an extreme example, the healthcare protection professional must engage hospital administration in a discussion of the advantages and disadvantage of each uniform style to facilitate a best decision for the organization. [Table 8-1](#) provides a brief overview of the advantages and disadvantages of each uniform style.

### *Function of the Security Staff*

What primary function the security department in general is carrying out, or more specifically, the function of the security officer is fulfilling, should be the greatest influencing factor in determining the uniform to be worn by security staff. The officer with primary foot patrol responsibilities who the organization wants to be highly visible will often wear a different uniform option than the officer whose primary function is greeting patients and visitor management. There are many uniform options for the healthcare organization to choose, with compelling arguments for each. The preferred uniform style is outlined in [Table 8-2](#) by the security function performed.

**Table 8-1** Advantages and Disadvantages of Security Uniform Styles

	Uniform Style		
	Traditional Military	Blazer	Polo
Visibility	Very Good	Fair/Poor	Good
Customer Friendly	Good	Very Good	Good/Fair
Professional Image	Good	Very Good	Fair/Poor
Comfort	Fair/Poor	Good/Fair	Very Good
Commanding Presence	Very Good	Fair	Good/Fair
Reassuring Presence	Good/Fair	Good	Fair
Inclement Weather	Very Good	Fair/Poor	Very Good
Armed	Very Good	Poor	Good

### *Traditional Military Uniform Style*

The vast majority of healthcare security officers are traditionally uniformed in a military- or police style uniform. Wearing this style of uniform readily identifies security staff and commands control when it is necessary to regulate behavior and provides a deterrent to criminal activity. The uniform is versatile—it can be worn indoors and outdoors in all climates. This style of uniform is preferred for officers who encounter many confrontational situations or primarily perform foot patrol. [Figure 8-1](#) is a picture of a sample traditional style uniform.

A traditional uniform can be softened in terms of color and style. For example, the visor cap, which strongly suggests a military and authoritarian role, is not part of many uniforms. Many programs prohibit hats within the facility, and some even prohibit hats outside the facility. Another example is the use of the commando style sweater.

**Table 8-2** Preferred Security Uniform Style by Function

Function	Preferred Style	Rationale
Foot Patrol	Traditional Military	Visibility/Deterrence/Respect
Bike Patrol	Polo	Functionality/Visibility
Greeter/Security Ambassador	Blazer	Customer Service Focus
Metal Detector Post	Traditional Military	Command Presence
Behavioral Health	Blazer	Reassuring Presence
Specialized Sitter	Polo	Patient Care Involvement
Security Dispatcher	Polo or Business Casual	Comfort/Image



**FIGURE 8-1** Sample traditional style uniform.

Frequently used in cooler climates, these sweaters can provide additional comfort to the security officer as well as soften their authoritative look without sacrifice of visibility. Many organizations have also introduced cloth badge patches, moving away from the more traditional metal badge. The cloth badge softens the look of the traditional uniform while enhancing officer safety and reducing uniform cost. In some healthcare protection programs, clip-on ties have been added to increase the professional image of this style of uniform. At Wheaton Franciscan–All Saints Healthcare in Racine, WI, the addition of the tie to the standard uniform issuance improved the overall image and significantly improved the perception of the security department by both patients and employees.

Name plates, badges, organizational issued identification, merchant guard licenses, supervisor insignia, and recognition pins are commonly found on the security officer uniform. Each serve an important purpose and can often be a source of pride for the officer. Care should be given to not crowd the uniform shirt with too much paraphernalia, presenting an unprofessional image. To distinguish supervisors from officers, many healthcare facilities have them wear a different color shirt—white for supervisors, blue for officers.

The style, color, and type of uniform are often controlled by local or state regulations. With or without regulation, the uniform should not be designed to replicate the uniform of any law enforcement agency. To prevent security officers from looking like law enforcement, the state of Arizona has forbidden the color blue to be prominent anywhere on the uniform. A hospital in Texas was accused by two legal aid groups of designing its security uniforms to look like the uniforms of US Border Patrol agents. A representative of the Texas Rural Legal Aid claimed that the hospital used the uniforms to discourage Hispanics from seeking medical care and thereby avoiding any violation of the Medicare anti-dumping law.<sup>1</sup>

### *Blazer (Ambassador) Uniform Style*

The blazer style uniform with contrasting slacks (gray slacks and blue blazer) can be a very professional look, and works best for officers who work mainly inside the facility and function primarily in a public relations mode. Many behavioral healthcare facilities prefer security officers working in these environments to work in the blazer style uniform to prevent the uniform from unnecessarily antagonizing patients or visitors. [Figure 8-2](#) is a picture of a sample blazer style uniform.

If blazers are worn, they should be designed so that security officers are readily identifiable. Without readily visible identification, poor public relations and unnecessary confrontations may result. Not a recommended practice, but if the blazer is removed during the course of duty, specific guidance should be given on how the officer is to be identified to the public.

The blazer style uniform does not offer the same flexibility as the traditional military style uniform. This style of uniform makes working outdoors in weather extremes difficult. Many licensing agencies prohibit security personnel from wearing this style of uniform and working in an armed capacity. Even in states where concealed carry weapons



**FIGURE 8-2** Sample blazer-style uniform.

(CCW) permits are issued, security staff wearing a blazer style uniform should never carry a concealed firearm.

### *Polo Style Uniform*

The high-visibility polo has become a fast growing non-traditional uniform option for an increasing number of healthcare security programs. Worn with slacks, battle dress uniform (BDU) style pants/shorts, or line uniform trousers, the polo shirt is typically identified with “SECURITY” on the back. This uniform option is frequently used for security officers who perform bike patrol functions. The expanded functionality of this uniform provides the officer with greater freedom of movement required by the bicycle and withstands more wear and tear than the traditional external patrol officer. These uniforms can also be used for armed security personnel. [Figure 8-3](#) is a picture of a sample polo shirt worn by healthcare security officers.

This style uniform is also worn by a growing profession in the healthcare protection industry—the *specialized sitter*. These staff members are frequently used to stand by and watch at-risk patients in a one-on-one situation for elongated periods of time. The polo style uniform is the most comfortable while allowing these employees to be a visible component of the protection program without provoking the patient. Additionally, this style of uniform does not have the many accoutrements normally found on the traditional military style uniform that could harm the employee or patient in the event verbal de-escalation attempts are unsuccessful and a hands-on approach to patient management is required.

The security dispatcher is often located outside of the public view. Outfitting dispatchers in this softer uniform style is usually done for the sole purpose of comfort in the work environment. A recent trend for many healthcare organizations employing security



FIGURE 8-3 Sample polo-style uniform.

dispatchers is to allow these employees to wear professional attire similar to other non-uniformed employees in the organization. This practice is not recommended for organizations that have dispatchers located in public view or share patrol functions or other duties with uniformed security staff.

Organizations may elect to adopt all three uniform styles in their protection programs: the regular security officers may wear traditional military style uniforms, bike patrol officers and specialized sitters may wear the polo style uniform, while supervisory personnel may wear blazers. Some job responsibilities may best be fulfilled by a traditionally uniformed officer, while for others, the blazer is preferred. For example, patrol and response officers might wear traditional uniforms, while fixed-post officers who perform an access control/greeting function might wear blazers.

## Supplying and Maintaining the Uniform

Because the uniform is such an important element in the operation of a security force, the organization should provide and, if possible, maintain the uniform. Ideally, officers should be required to report for duty in personal clothing and change into their uniform. In this system, the organization dry cleans or launders the uniform and prohibits officers from wearing the uniform off duty. This system is, of course, quite costly and is therefore not a widely utilized practice.

The US courts have interpreted the Fair Labor Standards Act (FLSA) wage and hour regulations to read that the officer must be paid for the time if required to change into the uniform on-site and not allowed to change at home. In *Lee v. Am-Pro Protective Agency, Inc.*, 860 F. Supp. 2d 325, 326 (E.D.Va.1994). The courts ruled that security officers are entitled to compensation for dressing into uniforms on-site where they were not allowed to change at home.

Organizations that provide uniforms for security personnel have more control over the quantity and quality of the uniforms. All too often, newly hired officers who must provide their own uniforms find the initial cost outlay a burden. As a result, they sometimes do not purchase enough individual uniform items to maintain a proper appearance.

There are alternatives to the organization's supplying the complete uniform. As a condition of employment, some security department require a uniform deduction to be withheld to offset the cost of uniforms if the officer resigns or is terminated within a specified time, usually 3 months. Other organizations hold a deposit until after separation of employment. Some state statutes do not allow either of these practices, so proper legal advice should be sought before implementing this practice. It is recommended that interest be paid on money held as a uniform and equipment deposit; in fact, interest may even be legally required. If money is withheld from an employee's paycheck to cover a deposit, the organization is limited in the amount that can be withheld from any given paycheck. The employee must be paid at least the minimum wage for the hours worked before a deduction can be made. [Figure 8-4](#) provides an example of standard employee authorization form used by many healthcare organizations that deduct uniform expenses from their employee's paycheck.

Another method of cost control is to require that security officers purchase their original uniform, while replacements are paid for by the organization. This procedure is effective in eliminating applicants who are seeking only temporary employment. One facility reports that it has been able to contain costs by not purchasing an outside jacket for each officer. The facility maintains a supply of jackets in various sizes. Officers select their jackets from the supply at the beginning of the shift when they draw their weapons and other equipment. This practice may help contain costs, but can also significantly

### UNIFORM DEDUCTION AUTHORIZATION

In connection with your employment, you are required to wear a uniform that has been purchased for your use. Uniforms are of substantial value and will remain the property of \_\_\_\_\_. It is your responsibility to keep this uniform clean and in good repair.

Please sign below to indicate that you agree to have \$50.00 deducted from your 2<sup>nd</sup>, 3<sup>rd</sup>, 4<sup>th</sup> and 5<sup>th</sup> paychecks (\$200.00 total) as a **security deposit** for the uniform. This deposit will be returned to you in full, provided the entire uniform is returned in good condition within seven days of the conclusion of your employment. A \$25.00 cleaning fee will be assessed if the returned uniform has not been dry-cleaned.

Upon resignation/termination, if you do not return all the uniform pieces, as listed on the Uniform Issue Form, in good condition or fail to return the uniform, you acknowledge that \_\_\_\_\_ will keep the deposit and can deduct from your paycheck or bill you later for the value of any damages, up to and including the full value of the uniform.

Print Name	Employee's Signature	Date
------------	----------------------	------

**FIGURE 8-4** Sample uniform deduction authorization language.

reduce employee morale. The healthcare security administrator should recognize the attire of security officers also influences their own attitude; attire that suggests an air of dignity and action tends to produce officers with those traits.

Larger security forces can reduce uniform costs by making use of existing uniforms. Regardless of the size of the force, returned uniforms represent dollars, and the supply should not be allowed to build up excessively. It is much more economical to expend money on alterations than to order new uniforms. Uniform rental firms also provide an alternative to hospital-owned and officer-owned uniforms. Uniforms should be clean when returned upon termination, and professionally dry-cleaned when appropriate. The failure to return hospital-owned uniforms in the appropriate condition should result in a predetermined deduction from the officer's final wages.

Facilities in areas with wide temperature swings often elect to provide both summer and winter uniforms for their staff.

## Use of Firearms

Whether security officers should be equipped with side-arms requires constant evaluation and reexamination. The answer is found in individual program needs, and the question cannot be answered with a simple yes or no. For program effectiveness and deterrent value, the preponderance of evidence supports armed security officers. However, armed officers may prove a detriment in various situations or functions rather than an asset.

Proponents of providing firearms for healthcare security officers argue that if an organization gives officers the responsibility of protecting life and property, it should provide them with the tools to do their job. Officers who can meet force with force can more efficiently carry out their responsibilities. Those against providing firearms often cite the liability involved and almost always stress a case in which a firearm was used inappropriately. Some opponents argue that security officers guard property and need not use deadly force. The firearm does nothing more than allow officers to protect themselves and others while they protect property. The value of property is significant only to the extent that it invites intruders. If security officers are expected to confront strangers, their personal safety must be paramount regardless of property value.

At present, approximately 12 percent of US healthcare security officers are armed.<sup>2</sup> When the previous edition of this book was published in 2001, about 15–20% had firearms, down from 30% in 1992. Thus, the trend appears to continue toward unarmed security officers. However, security managers must make the correct decision in regard to firearms for their particular circumstances, and must not simply follow a trend.

## Considerations in Arming Officers

The correct decision on whether to arm security officers for a given organization requires consideration of many different factors. Among these considerations are personal safety, vulnerability, liability, deterrent value, environmental profile (status of the neighborhood, geographical setting, degree of crime in and around the facility), and quality of personnel.

### *Personal Safety*

Personal safety is, of course, the central issue in whether to arm officers. The people at risk can be divided into the protection of officers themselves and the principals (employees, patients, visitors) they are protecting. Armed security officers feel safer as their ability to protect themselves increases. No amount of judo or other alternatives can match an opponent with a firearm. Conversely, officers are sometimes safer without a weapon. If a security officer is obviously not armed, a foe need not use deadly force to accomplish his objective. The persons that the security officer protects have a greater feeling of security when the officer is armed. Thus firearms provide both officers and those they protect with a sense of security, regardless of the real need for firearms.

### *Vulnerability*

The degree of vulnerability that the officer and the organization face is also an important consideration. In larger acute-care hospitals, the quantities of drugs and money and the number of serious assaults are considerably different from those found in small suburban or rural facilities. The degree of vulnerability also varies in relation to the environmental setting. For the individual officer, vulnerabilities also vary considerably. A security officer patrolling warehouses and parking lots at 3:00 A.M. is in a different position from that of an officer assigned to an access control point within the facility. Generally, fewer security staff are armed in programs that are primarily internal than in programs that must deal with a campus and so-called street problems.

### *Liability*

Potential for legal liability actions is greatest with armed officers. Officers who misuse their weapons can create a liability, as can a nurse who misuses a needle when injecting a patient. However, an unarmed officer who cannot effectively prevent injury to a patient, visitor, or employee, might create a liability of a different nature. The problem is that one cannot know whether the firearm helped avert an incident that might have led to a liability claim.

There is one approach to providing firearms protection to the healthcare center without arming any of the regular security staff: hire off-duty law enforcement officers. Although this is an expensive approach, the healthcare center can avoid the training issue and a certain degree of liability. What may be wrong with this approach is that training and liability may not be avoided at all, as the selection of the specific officer working the off-duty post is often outside of the control of the organization.

An example of what can go wrong when off-duty police officers work at healthcare facilities can be found in the case of *Melendez v. City of Los Angeles*. In this case, two off-duty police officers working at the facility were involved in an altercation in which a person was shot. The healthcare facility that had hired the off-duty officers avoided a court decision by settling out of court for \$550,000. However, a jury found the city liable for \$10,212,500, in part because it thought the city was guilty of negligent retention of one of the officers, who had allegedly been involved in other incidents in which excessive force was used. In addition, the jury found that the police officers were acting within the scope



of their employment as law enforcement officers at the time of the shooting, despite the fact that they were “off duty.” This particular case is not unique. The issue of off-duty police officers working for private organizations deserves serious attention by private organizations and law enforcement agencies alike.

### *Deterrent Value*

One of the strongest arguments in favor of arming security staff is the preventative value of firearms. One can only assume that most serious crimes are planned to some degree, and that part of that planning is to select a target in which armed security officers will not be encountered.

### *Environmental Profile*

The type of neighborhood, together with the associated level and type of crime, must be analyzed in determining the need for armed security personnel. A quiet residential setting with an older population presents far different issues than a rundown commercial or transient community. In reviewing the crime status of the area, the number of crimes as well as the seriousness of the crimes is important. In this respect, a high number of minor crimes can suggest that more serious crime is foreseeable, providing there is a linkage. An example is a person stealing car parts in a parking lot that is interrupted and violence results during an attempted escape. An escalating level of minor crimes is often the forerunner of increasing violence and crimes against persons.

In addition to police crime statistics, CAP Index CRIMECAST reports should be used to identify the risk potential of criminal activity on campus and the surrounding neighborhood. The model builds upon the strong relationship between a neighborhood’s “Social Disorder” and the amount of crime perpetrated there. By combining surrounding social characteristics, survey information and other databases with known indicators of crime, the CRIMECAST® model is able to provide precise scores indicating a site’s risk of crime in comparison to national, state, and county averages. [Figure 8-5](#) illustrates a sample CRIMECAST Site Data and Map.

Generally when a healthcare organization makes the decision to go with armed security personnel, they do so because of aforementioned neighborhood demographics information but also take into consideration the degree of crime in and around the facility and police response time.

If available, the healthcare facility should ascertain the local Police Department statistics on crime for the hospital and the crime reporting area, grid, or zone in which it is located. In most cases, these statistics are tabulated monthly and can be obtained at no charge or for a nominal fee. Often crimes reported from the hospital actually occur elsewhere; they are simply called in to 911 by the victim or medical personnel, usually from the emergency department. This is why it is essential to correlate police crime statistics with hospital incident reports to determine if a crime actually occurred on campus.<sup>3</sup>

Reviewing the statistics with the local community resource officer can also serve to be an invaluable exercise. Often, these representatives of the agency having jurisdiction



**CRIMECAST® SITE REPORT**  
PREPARED BY CAP INDEX, INC.

Scores indicate the risk of crime at a site compared to the average of 100 (i.e. A score of 400 means that the risk is 4 times the average and a score of 50 means the risk is half the average).

Current Scores	National Scores	State Scores	County Scores
CAP Index	686	1156	469
Homicide	248	452	329
Rape	409	1000	428
Robbery	798	1249	495
Aggravated Assault	327	763	440
Crimes Against Persons	461	940	455
Burglary	554	923	449
Larceny	529	748	435
Motor Vehicle Theft	158	294	197
Crimes Against Property	437	658	374

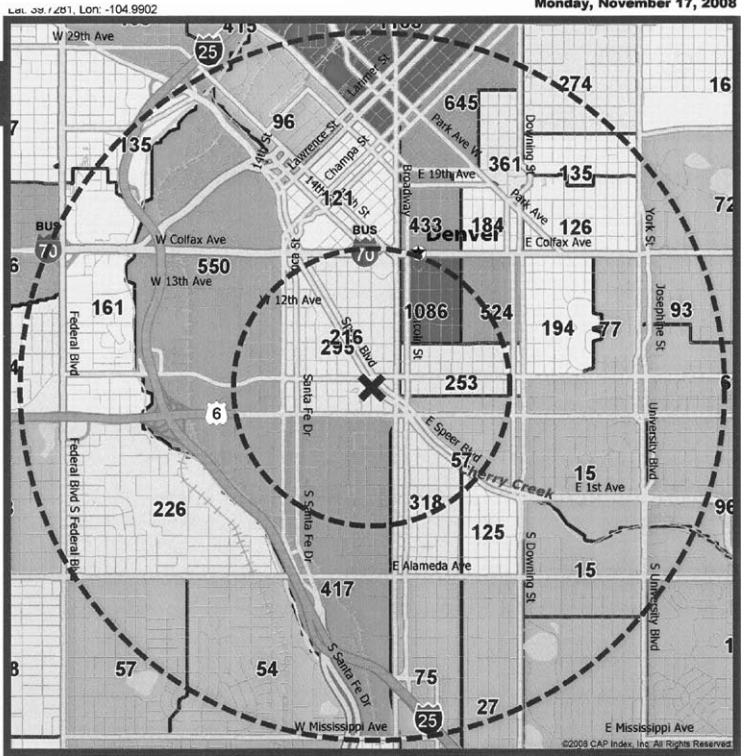
CAP Index	National Scores	State Scores	County Scores
Past - 2000	660	1181	475
Current - 2008	686	1156	469
Projected - 2013	725	1219	511

Notes:

.....  
 .....  
 .....  
 .....  
 .....  
 .....  
 .....

**National CAP Index = 686**

**CRIMECAST® Standard Report**  
Monday, November 17, 2008



Underlying map data derived from MapQuest and/or MapQuest services.  
 CRIMECAST® is a trademark of CAP Index, Inc. Please note terms and conditions as presented on <http://www.capindex.com/terms.html>

FIGURE 8-5 Example of a CRIMECAST map and site date (Courtesy of CAP Index, King of Prussia, PA).

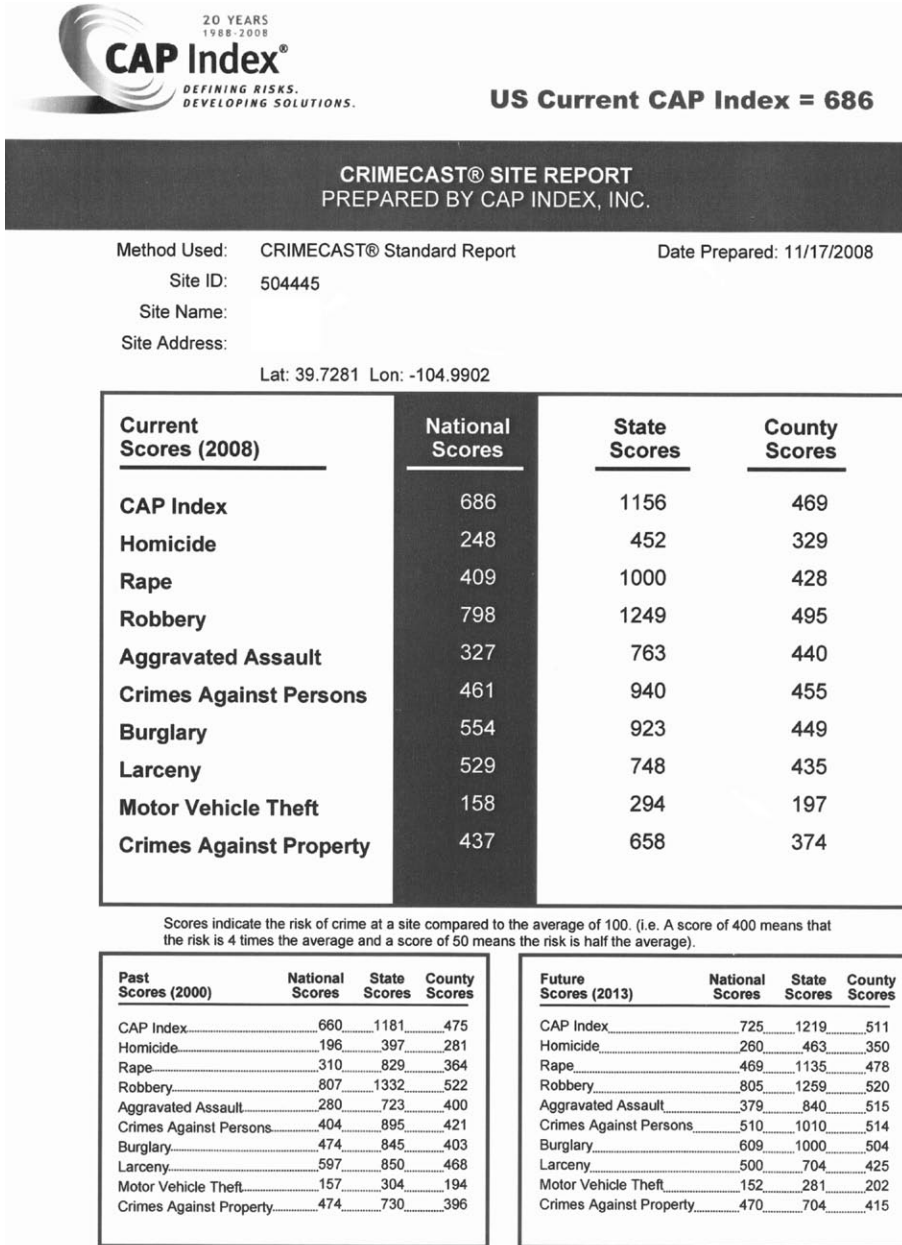


FIGURE 8-5 (Continued)

can help identify changes in the community, provide a broader understanding of trends in the neighborhood, and provide an understanding of how much police presence the department provides to the medical center.

The objective nature of healthcare security and police crime statistics, coupled with a CAP Index report, provide evidenced-based considerations when evaluating the decision on the need for armed security officers in the healthcare environment.

### *Past Experience with Weapons*

The presence of illegal weapons on campus is an important indicator in determining the need of armed security personnel. The healthcare organization should ask a few essential risk-based questions when evaluating the need for an armed security presence, or disarming current staff, that includes a comprehensive review of past experience on campus related to:

- Discovery of weapons brought into the facility?
- Discovery of weapons found on campus?
- Incidents where security officers used weapons in the course of duty?
- Incidents where weapons may have been needed?

Weapons are often found when metal detectors are used to screen persons entering emergency departments.<sup>4</sup> A 4-year study at Henry Ford Medical Center, Detroit, MI, reported that 4 percent of people arriving at their emergency department carried weapons to some points in the hospital.<sup>5</sup> A 3-month look at three Level I trauma centers in Denver, CO, employing magnetometers in their emergency department protection efforts found an unexpected quantity of commandeered items. During the period, one facility confiscated 434 banned items, including three guns. Another took possession of 558 banned items while a third confiscated over 1,200 prohibited objects, with an average of 25 to 30 illegal knives each month. For these three facilities, the volume of illegal weapons confiscated (both firearms and edged weapons) was a significant factor in determining the need for armed security.

### *Community Standard*

Another important consideration when evaluating the use of armed personnel is the community standard. The assessment should include a detailed understanding of the use of armed security at other healthcare facilities in the region. Identification of this “tipping point issue” is an important consideration before making a change.

For 20 years, trends indicate that a large volume of healthcare organizations have transitioned to an unarmed security model. If a healthcare facility in the region has recently disarmed their security staff, efforts should be made to glean information relative to the decision. Did they have a significant event, or close call, that brought the issue of armed staff to the surface or was there merely an administrative change in preference?

Gaining knowledge of the rationale at other healthcare facilities for using an armed (or unarmed) security model can provide significant insight into the decision matrix.

The community and patient demographics differ by facility; no two healthcare environments are exactly alike. However, physicians often have privileges at multiple hospitals and healthcare has a large transient workforce who frequently job hop in search of better schedules, shorter commutes, and safer work environments. The knowledge of the model of security in place at other healthcare facilities alone can help stem off negative perception of the protection efforts on campus. All too often, the rationale received is security staff “have been armed since I have been here” and no one has ever questioned the rationale. Unfortunately, many healthcare organizations never review the issue unless a significant event occurs because “it’s just the way it’s always been done.”

#### *Circumstances for Officers to Disarm*

Many organizations also have protocols on the circumstances for when armed personnel must disarm while performing certain duties. Security and law enforcement have been prohibited from carrying their firearms onto most behavioral health units for years. With the continued trend of reduced behavioral health care funding in the United States as illustrated with the large number of closing of many primary mental healthcare facilities and inpatient units, the emergency department is flooded with a growing number of mental health patients. Often, the patients present to the healthcare facility with an even greater level of acuity than before. As a result, a number of emergency departments have given great consideration to requiring their security officers and even gone so far as requesting law enforcement to disarm before entering the medical treatment area of the emergency department.

The simple act of disarming creates a litany of issues from gun locker storage location to additional training requirements to prevent accidental discharges when the firearm is handled in the public arena. The preferences and specific risks must be taken into consideration when evaluating the use of armed security personnel.

#### *Quality of Personnel*

Many times the problem is not whether a security officer should be armed; it is the availability of competent, well-trained security officers available to carry firearms. No amount of pre-service or in-service training can compensate for security officers who do not possess the aptitude to practice the training provided.

Regardless of what kind of prior training a security officer has been provided historically—e.g., post certified or previous company training—every organization should require that the security officer complete its NRA-certified training program. This training should preclude any security officer from carrying a gun on duty unless he/she has fulfilled the competency training standard and firing range proficiency. The quality of the program and the authority of the instructor to eliminate those officers who should not carry firearms is paramount.

#### *Type of Weapon, Holster, and Ammunition*

The decision to use firearms in a security program mandates additional management responsibility and adds to costs. A major decision that must be made concerns the type

of weapon, holster, and ammunition to be used. These decisions are sometimes determined by licensing laws.

Whenever possible, the organization should furnish the weapon, and it is preferable that weapons be checked in and out for each tour of duty. Where economics and other operational factors preclude the organization from owning the weapons, basic standards must be established for officer-furnished weapons and ammunition.

The type of holster to be used is another important consideration. Security personnel should only be allowed to carry a Level I, II or III safety holster. It must ride close against the body and be difficult for another person to remove the weapon from the officer. Too many security officers have been shot with their own weapons after losing them to an assailant. Healthcare security officers should never be allowed to carry concealed weapons (even with a concealed weapon permit) while performing hospital services. Not only is this practice evidence of a poor management decision, it can also have serious consequences in terms of public relations and liability issues.

## Trends in Arming Security Personnel

To reduce liability while providing the security system with a limited weapon capability, some programs arm only the supervisory staff. This approach is predicated on the reduced exposure of weapons and the fact that supervisory personnel are generally better trained and more capable of properly handling weapons.

Another approach is to arm those officers who are assigned to external patrol and to eliminate firearms for those personnel assigned to the emergency department, behavioral health, or other departments commonly found with at-risk patient populations. If walk-through metal detectors are used, this model is often augmented with arming the security staff assigned to this post.

Whether to arm security officers or not is a grave decision that must be made with deliberation. There is always a risk, and the decision must be made on the basis of this question: Does the weapon provide enough benefits sufficient to offset the liability and cost involved?

## Managing the Firearms Program

A firearms policy is mandatory. The policy must be clear, concise, and understood by every officer. A firearms weapon affidavit should be completed by all officers who carry firearms. [Figure 8-6](#) is an example of such a firearms affidavit. The affidavit could be further expanded to serve as the administrative policy.

It is often claimed that a weapon should not be taken from a holster unless it will be used, and that one should never fire a weapon in the air. However, a drawn weapon might be appropriate in some instances, for example when answering an intrusion alarm in a closed pharmacy or when interrupting a crime in progress and ordering suspects to raise their hands. Firing in the air is considered to be inappropriate.

**WEAPON USE AND SAFETY AFFIDAVIT**

1. The weapon you carry in the performance of your duty is for the protection of life. Deadly physical force may be used only as a last resort if the Security Officer reasonably believes a lesser degree of force is inadequate, and; the Security Officer has reasonable grounds to believe, and does believe, that he or another person is in imminent danger of being killed or of receiving great bodily harm.
2. All weapons are dangerous, it is mandatory that the Security Officer treat his weapon with care, respect, and remembering that at all times handling the weapon safely is the most important requirement.
3. The person with a firearm in his possession has a full-time job. You cannot guess—you cannot forget. You must know how to use, handle, and store your firearm safely. Do not use any firearm without a complete understanding of its particular characteristics and safe use. There is no such thing as a foolproof gun.
4. From the time you pick up a gun you become part of a system over which you have complete control. You are the only part of the system that can make a gun safe or unsafe.
5. Firearms will not be removed from the holster or otherwise drawn unless there is an immediate threat of death to the officer or other persons present. The firearm will not be removed from the holster for show or display or at the request of other security personnel. Security Supervisors are entitled to inspect the gun to determine the cleanliness of the weapon and whether you are carrying appropriate ammunition.
6. Warning shots will not be fired under any circumstances.
7. I will never leave a loaded firearm where someone else may handle it. When not on my person, my weapon will be secured. This includes at work, traveling to and from work, and at home.
8. The officer must carry the firearm and ammunition that was approved by the local law enforcement agency. Carrying a weapon or ammunition other than that approved is forbidden and could result in termination.
9. The weapon must be cleaned after each shooting session; failure to do so could result in a malfunction of the weapon.
10. Alcohol, drugs, and guns don't mix. Do not handle firearms if you have been using alcohol or are under a doctor's medication containing narcotic derivatives.
11. Do not shoot at or from a moving vehicle. If you disable a driver you have now created a 3,000 pound missile capable of inflicting serious injury or death to an innocent party.
12. I understand that the license issued to me prohibits my wearing the uniform and/or weapon while off duty except to travel directly to and from home. The weapon must be secured in the trunk or placed in a container out of public view.
13. Don't be timid when it comes to gun safety; if you observe anyone violating any safety precautions, you have an obligation to suggest safer handling practices.
14. Any time you pick up a weapon my must adhere to the following practices:
15. Point the gun in a safe direction.
  - a. Visually inspect the gun to be certain that the gun is loaded or not loaded. Count the cartridges.
  - b. When not in actual use, firearms must be unloaded.
  - c. Never touch the trigger on a firearm until you actually intend to shoot.
  - d. You must be able to identify your target and what's beyond it.
16. All security personnel shall strictly adhere to this order. Violations of policies set forth herein will result in disciplinary action. This policy shall be effective at all times regardless of location.

PRINT NAME \_\_\_\_\_ SIGNATURE \_\_\_\_\_ DATE \_\_\_\_\_

WITNESS \_\_\_\_\_ DATE \_\_\_\_\_

**FIGURE 8-6** Example of a security officer firearms affidavit training (Courtesy of HSS Inc, Denver, Colorado).

Firearms training is an essential ingredient in properly managing an armed security program. This training must be an ongoing program of classroom instruction and firing range experience. All armed officers should fire on the range at least once—and preferably twice—each year.

Training instructors should be carefully selected for two reasons. First, the highest level of instruction possible should be provided. Second, the qualifications of the instructor and the quality of the instruction can be of prime importance in any litigation alleging misuse of a firearm by a security officer. The instructor should be qualified by the National Rifle Association (NRA) to teach the police and security program. The minimum requirement for the firearms instructor should be attendance and successful completion of the NRA 44-hour tactical handgun course which entitles the instructor to conduct courses for both police and security personnel.

## Other Equipment Considerations

A security officer can carry only so much equipment, and the security administrator must decide which equipment is most necessary for a particular system. Officers so loaded down with equipment that they have difficulty moving freely exhibit a poor image. The needs of each program will vary. The following equipment list is offered only as a guide:

- Notebook and Pen
- Communication Devices
- Handcuffs
- Flashlight
- Personal Protective Equipment (PPE)
- Tasers (Electronic Control Devices)
- Chemical Agents (irritants)
- Batons
- Protective Vests
- The Duty Belt

Although not categorized as equipment, a nameplate or other identification consistent with the facility's overall employee identification plan should be worn by all officers. Equipment that is generally unnecessary includes whistles and items such as knives and novelty weapons.

### Notepad and Pen

Often overlooked, a security officer should never be allowed on a post or patrol without a notebook and writing instrument. It can be a healthcare security officer's most-used equipment. Small enough to fit into the security officer's pocket, the notepad can be used to capture investigative notes and contain needed information such as emergency codes for the facility and radio codes for the department. Some departments even provide their security staff with foldout maps of the facility grounds and security incident report drafts that can help with key questions to ask during simple and complex investigative activity.



## Communication Devices

The most important piece of equipment a security officer can carry is the two-way radio, which is part of the overall security communications system. A one-way pager is simply unacceptable. Not only does the radio provide an element of personal safety for the officer, but it is essential in achieving an effective security system. However, many facilities expend thousands of dollars for security personnel and fail to spend a small amount to achieve a 50–100% increase in effectiveness through improved communications. Archived reports attest to the success of radio communications in saving lives, preventing total-loss fires, and apprehending criminals of all types. Radios create a deterrent value when used by a lone security officer confronting a hostile individual(s). A call for assistance alerts the hostiles that help is on the way.

Radio equipment is available in all shapes and sizes and with varying states of sophistication. Many large and well-funded departments use wide-area radio networks or repeater systems for officers to communicate with one another and to hear broadcasts from the central station. This traditional two-way radio communication is still preferred by most healthcare protection professionals. Advanced two-way radios have multiple channels, one or more of which can be used for supervisory personnel. This allows security leaders to have private conversation so they can discuss sensitive subjects. The text messaging feature available on many radios can also keep communication confidential.

Advanced communications systems available from suppliers such as Sprint/Nextel Direct Connect have grown in popularity. Providing the ability for officers in the field to link with three independent forms of communication—cell phones, radio, and text messaging, this technology application provides significant redundancy in critical communication for security staff. Preferred for multiple campus locations and smaller departments, signal strength can be amplified inside the healthcare organization for a fraction of the cost of a wide-area radio network.

Some radios have *call alert* and *selective call* features that can page a specific person or group during an emergency, such as an evacuation, power failure, or patient emergency. Call alert or selective call allow these situations to be managed by appropriate personnel without disturbing other users who are not involved. The GPS option available on many of the newer radios enables the security officer to communicate due to an accident or assault, or for management to locate that individual to render assistance. The location of each security officer can be displayed on the dispatcher's computer screen for officer safety and asset management.<sup>6</sup>

Good communications equipment is expensive; however, the cost has come down in recent years. Considering the life of today's equipment, the cost, depreciated over the number of usable years, is the best investment of security dollars that an organization can make.

Limited two-way radio codes in security operations can be useful in reducing valuable airtime. The 10 codes that were once popular have generally been found to be of limited value and have sometimes caused more problems than no codes at all. Most law enforcement agencies and security departments have eliminated the 10 codes except for a few basic codes.

Several problems are inherent in any code system; chief among them is the training required. With a constant turnover of personnel, the training issue assumes major proportions. Another problem is that the codes cannot cover the diversified and sometimes specific information that must be communicated. Field analysis has shown that departments that use extensive code systems do not necessarily use less airtime than do departments that have eliminated their codes. The main items of concern in radio transmission are minimal airtime and clarity (understanding) of the message being transmitted. Both of these goals can be adequately achieved by simply stating the message in concise, everyday language.

## Handcuffs

Handcuffs are an important piece of equipment carried by many healthcare security officers. Security officers may need to use handcuffs for maintaining custody and control of persons arrested, as well as for detaining persons who exhibit behavior that may be harmful to themselves or others.

In restraining out-of-control patients, regular medical restraint devices will generally be utilized. Historically, there have been occasions when the security officer's handcuffs may have been used as the most expedient means of temporarily maintaining patient control. However, the Centers for Medicare and Medicaid Services (CMS) does not consider the use of handcuffs or other restrictive devices in the application of restraint or seclusion as a safe, appropriate health care intervention.<sup>7</sup>

Handcuffs and flex cuffs can be very useful tools but their use should be documented and governed by the hospital's patient restraint policy. CMS is very specific about the use of handcuffs in the patient restraint process and although they do not outlaw their use, they do outline a specific response that includes immediate notification of law enforcement personnel. In short, CMS does not want to see handcuffs used in the patient restraint process unless an arrest is imminent. As a result, many healthcare organizations have re-evaluated handcuffs and flex cuffs for their usefulness and application in the hospital setting. An increasing number of hospitals have forbidden security officer from carrying handcuffs to prevent inappropriate use.

The healthcare organization and security administrator should carefully consider the use of handcuffs as the security officer will frequently use them when responding to major disturbances and other out-of-control situations. In one such situation, officers were called to a medical center parking lot on reports of a man kicking and screaming inside a parked vehicle. As the security officer approached the vehicle, the man exited it and charged the officer. A struggle ensued, and with the help of a second officer, the man was controlled with handcuffs. The man quit struggling as soon as the handcuffs were applied, and one of the officers discovered that the man had stopped breathing. Medical assistance was immediately summoned and CPR was initiated. Unfortunately, in this case the man died, and the police began an investigation.

In the initial stages of the investigation, a little-known phenomenon called Sudden In Custody Death Syndrome (SICDS) was found. The majority of SICDS cases involve

respiratory difficulties brought on by a variety of factors that lead to asphyxia. Asphyxia refers to either reduced oxygen or elevated levels of carbon dioxide and leads to the body tissue not getting sufficient oxygen.<sup>8</sup> Persons who are on drugs, abuse alcohol, have a mental illness, or are obese are at greater risk for asphyxia in stressful situations. In physically restraining persons, officers should not leave them on their stomach any longer than necessary or apply weight to their back or chest (compressing the rib cage). In addition, officers should be cognizant that a person's resistance to physical control may be a struggle for oxygen as opposed to continued resistance to the restraint. In a review of twenty-one cases where patients died unexpectedly while being physically restrained, the prone position was associated with each case.<sup>9</sup>

Quality handcuffs are a necessity. In some embarrassing instances, handcuffs had to be cut off a person due to a malfunctioning lock. All handcuffs carried by security officers should operate with the same type of key. Because handcuffs reinforce the police image, they should be completely enclosed within a leather case rather than carried exposed. The line inspection discussed in *Chapter 7, Security Force Administration*, should include a physical examination of the officer's handcuffs on a routine basis.

## Flashlight

A flashlight should be carried by all security officers, regardless of working during the day or at night. It is the piece of equipment most often found lacking when reviewing officers in the field. The reluctance to carry a flashlight may be due in part to its size and weight. The new LED flashlights offered today are more compact than the older two- or three-cell "C" battery flashlights commonly carried by security staff (and often the source of reluctance for carrying). Today's lights have a tactical level output that is also far superior to the older styles. Larger flashlights or lantern-type lights can be stored for special use.

## Personal Protective Equipment (PPE)

The use of gloves in the healthcare setting has escalated in the past few years for all staff working in patient care delivery systems. One organization alone, the Mayo Clinic in Rochester, MN, reports using an estimated 10 million pairs of gloves per year. The advent of AIDS and mandates by the Occupational Safety and Health Administration (OSHA) have made the glove a major supply item in the healthcare environment. Gloves offer protection against the transition of disease and have thus become a primary item to be carried by the healthcare security officer.

Gloves are the most common type of Personal Protective Equipment (PPE) used in healthcare settings. However, it is reported that as many as 17% of healthcare workers have latex allergies—some so severe they have been forced out of their careers. In addition, powdered gloves create a source of airborne allergen that circulates freely through the air. The use of non-powdered gloves, gloves with a low latex level, or non-latex gloves should be considered in equipping security personnel.<sup>10</sup>

Gloves should fit the user's hand comfortably—they should not be too loose or too tight. They also should not tear or damage easily. Gloves are sometimes worn for several hours and need to stand up to the task.

OSHA standards for healthcare workers on Blood Borne Pathogens and Tuberculosis provides specific guidance to assist the healthcare security administrator in knowing what other PPE should be provided to security staff. Examples beyond gloves are:

- Goggles to protect the eyes
- Face shields to protect the entire face
- Gowns/aprons to protect skin and/or clothing
- Masks and respirators to protect mouth/nose and the respiratory tract from airborne infectious agents

Under OSHA's General Duty Clause, the healthcare security administrator should recognize that PPE is required for any potential infectious disease exposure. When selecting PPE, there are three key things that should be considered<sup>11</sup>:

1. *The type of anticipated exposure.* This is determined by the type of anticipated exposure, such as touch, splashes, or sprays, or large volumes of blood or body fluids that might penetrate clothing. PPE selection, in particular the combination of PPE, also is determined by the category of isolation precautions a patient is on.
2. *Durability and appropriateness of the PPE for the task.* This will affect, for example, whether a gown or apron is selected for PPE, or, if a gown is selected, whether it needs to be fluid resistant, fluid proof, or neither.
3. *Fit.* How many times have you seen someone trying to work in PPE that is too small or large? PPE must fit the individual user, and it is up to the healthcare organization to ensure that all PPE are available in size appropriate for the workforce that must be protected.

Security staff must learn to use PPE when a disaster strikes. The *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* recognizes emergency room workers as major responders to the problem of terrorism, and it promotes a national curriculum of training to respond to biological agents. Security staff fall under this guidance and need personal protection and training so they do not become victims themselves. As first receivers treat victims, security officers will likely maintain order and control traffic and access by victims who may be in a state of panic and need to be decontaminated and quarantined. Security staff must understand the PPE available to them and be properly trained on how to safely don and remove them if such circumstances should arise.

## Tasers (Electronic Control Devices)

While firearms can save the life of a healthcare security officer, they can also be dangerous to the person using them for protection, such as getting into the hands of the opponent. For this reason, many healthcare security programs have resorted to alternative means of

protecting security staff other than firearms in the security program. The Taser electronic control device has become an increasingly popular, less-lethal protective weapon. Tasers are weapons designed to incapacitate a person from a safe distance while reducing the likelihood of serious injuries or death.<sup>12</sup> Different from other less-lethal weapons such as chemical agents, Tasers do not solely rely on pain compliance. They affect the sensory and motor functions of the nervous system to achieve incapacitation.<sup>13</sup>

The weapon can be used from distances greater than those needed to use an aerosol spray allowing the deploying officer not to have to go hands on with the opponent. In addition to looking and handling like a gun, the Taser can be controlled by the officer. Unlike other use of force options, the effect ends at the moment the Taser's 5-second cycle is completed.

Safety is an important factor in the use of Taser guns in the healthcare setting. When deployed, the use of spotters is highly recommended to prevent the assailant from falling, a more common cause of injury than deployment of the Taser. However, getting in close enough proximity is not always possible.

Use of Tasers has dramatically increased over the past decade and are commonly used by law enforcement agencies within the United States as a complement to their firearms. In contrast, many healthcare security programs have displaced the firearm with the Taser. The device is considered a more suitable less-than-lethal option if an escalated use of force tool is warranted. The November 2007 IAHS/GE Security survey of 579 US hospitals illustrated that 16% of hospital security departments arm their security officers with Tasers compared to the aforementioned 12% for firearms.<sup>14</sup>

Most healthcare protection professionals agree, the less-lethal use of force option provided by the Taser is a better tool than the firearm to combat most escalated situations confronted by the healthcare security officer. Many healthcare emergency departments have requested for the Taser to be carried by hospital security departments, as the mere presence of the weapon on the side of a security officer has been found to de-escalate physically acting out patients who have not succumbed to more traditional de-escalation techniques. However, this practice is closely scrutinized by CMS and must be carefully monitored. CMS Interpretive Guidelines §482.13(e) states:

*The term "weapon" includes, but is not limited to, pepper spray, mace, nightsticks, Tasers, cattle prods, stun guns, and pistols. Security staff may carry weapons as allowed by hospital policy, and State and Federal law. However, the use of weapons by security staff is considered a law enforcement action, not a health care intervention. CMS does not support the use of weapons by any hospital staff as a means of subduing a patient in order to place that patient in restraint or seclusion. If a weapon is used by security or law enforcement personnel on a person in a hospital (patient, staff, or visitor) to protect people or hospital property from harm, we would expect the situation to be handled as a criminal activity and the perpetrator be placed in the custody of local law enforcement.*

St. John's Hospital in Springfield, MO, discontinued having their safety and security officers carry Tasers after the hospital examined the CMS regulations.<sup>15</sup> CMS has

threatened to pull funding from at least one hospital for improper use of Tasers. CMS officials found that psychiatric patients at Martin Luther King Jr./Drew Medical Center in Los Angeles were in “immediate jeopardy” of harm because police officers assigned to the facility were using Tasers and leather restraints to control them. A federal report released details of eight cases where Tasers were used at the hospital.<sup>16</sup>

The use of Tasers is not without critics. The Canadian Medical Association published an editorial in its May 20, 2008, journal calling for healthcare professionals to exclude themselves from using Tasers—calling for randomized testing of Taser guns and subjecting the devices to more objective, rigorous, and independent scientific testing standards and research.<sup>17</sup>

Emergency medical service providers are seeing more patients who have been subjected to the application of a Taser. An independent study assessing 1,201 patients who had been injured from Tasers found serious injury occurred in only 3 patients. No cardiac dysrhythmias associated with the Taser were documented.<sup>18</sup> Data shared in a study of 75 cases of Taser-related deaths found that sudden deaths can and do occur after Taser use. A common factor in these deaths is extreme agitation, often in the setting of stimulant drug use and/or preexisting heart disease. However, no conclusive direct link to fatal injury has been made.<sup>19</sup>

Every use of force by security staff involves some liability and litigation risk. For the healthcare organization, they should take responsibility for developing a specific use of force policy and training related to the use of Tasers. This should include specific deployment and postdeployment policies and procedures. Hospital policy on the use of force should incorporate restrictions outlined in [Figure 8-7](#) and reference the CMS interpretive guideline noted above.

## Chemical Agents

Chemical agents are quite popular in security work; approximately 20–30% of hospital security departments employ chemical agents,<sup>20</sup> with mace and pepper spray being the most commonly carried agents. There are other distinct types of gases: CN gas, CS gas, and oleoresin capsicum (OC spray), a pepper spray commonly used by law enforcement agents and security officers in Australia.

Each of these chemical irritants is a non-lethal alternative that can only be used when a security officer is in close proximity to an assailant. Emitting a liquid mix of chemicals, or peppers in the case of capsicum, the intention is to momentarily blind a person and cause temporary pain and discomfort when sprayed in an assailant’s face. The use of these canister-type sprays is legal in most states and countries.

Research indicates that the effectiveness of chemical agents is somewhat limited by the need for direct eye impact to achieve a rapid reaction. Studies also show that severe skin pain starts within 3 seconds and last for about 5 to 6 minutes. In addition, there is some question as to the effects of chemical irritants on different types of people. In some cases, no chemical agent will be effective on people under the influence of alcohol or drugs, emotionally disturbed or by focused, combative individuals. People must be able to feel or react to pain for the chemical agent to be effective.

Due to fear of contaminating inpatient units, many hospitals prohibit the use of chemical agents in their use of force continuum. The concern is if the chemical agent gets into the heating, ventilation, and air conditioning (HVAC) system, the hospital may be forced to evacuate the patient care area. The risk of contamination has been lowered by using pepper foam, which also carries health risks for people who have medical conditions

## TASER USE AND SAFETY AFFIDAVIT

Security personnel who have been trained to carry the X26 Taser **MUST** adhere to the following Policies and Procedures.

1. Before going on duty the X26 Taser and the holster must be carefully inspected to ensure that the device is fully charged and operational according to specifications, and the holster is in such condition as to provide for the security of the device.
2. The security of the X26 Taser is the responsibility of the officer to whom the device was assigned. Under no circumstances shall the officer leave the device unsecured. The X26 Taser, in the wrong hands, could represent a serious threat to innocent persons in a healthcare setting.
3. If the X26 Taser is damaged during the officer's shift, a Security Incident Report must be written documenting the nature of the damage and how the damage occurred. This information must be given to the shift supervisor before the end of the shift or the security supervisor at the earliest practical time.
4. Officers must carry the X26 Taser with the safety slide in the SAFE position.
5. The X26 Taser is a device of last resort. T.E.A.M. (Techniques for Effective Aggression Management) should be employed whenever appropriate, unless the subject becomes physically aggressive and represents a threat of injury to persons present. If it becomes apparent to the officer that the subject's behavior is escalating, always call for assistance. A show of force is often the best way to restrain aggressive behavior. The X26 Taser may be used when physical force is legally justified to prevent the reasonable foreseeable threat or actual attempted assault, battery, and/or injury to officers, other persons, and/or the subject. When practicable, avoid prolonged or continuous exposure(s) to the Taser device electrical discharge. The stress and exertion of extensive repeated, prolonged, or continuous application(s) of the Taser device may contribute to cumulative exhaustion, stress, and associated medical risk(s). Severe exhaustion and/or overexertion from physical struggle, drug intoxication, use of restraint devices, etc. may result in serious injury or death. The Taser device causes strong muscle contractions, usually rendering a subject temporarily unable to control his or her movements. Under certain circumstances, these contractions may impair a subject's ability to breathe. If a person's system is already compromised by overexertion, drug intoxication, stress, pre-existing medical or psychological condition(s), etc. any physical exertion, including the use of a Taser device, may have an additive effect in contribution to cumulative exhaustion, stress, cardiovascular conditions, and associated medical risk(s). To minimize the risk of injury, consider the following:
  - a. Begin restraint procedures as soon as it is reasonably safe to do so in order to minimize the total duration of exertion and stress experienced by the subject. Avoid touching the probes and wires and the areas between the probes during Taser electrical discharge.
  - b. If a Taser device application is ineffective in achieving the desired effect, consider reloading and redeploying or using other force option(s).
  - c. If a subject is exhibiting signs or behaviors that are associated with Sudden In-Custody Death Syndrome, consider combining use of a Taser Device with immediate physical restraint techniques and medical assistance.

Great justification must be provided when the X26 Taser is used against a pregnant female, children, seniors, restrained subjects, and passive individuals who are being arrested. Only when these subjects represent a serious threat of injury to the officers or others should the use of the X26 Taser be considered. The X26 Taser may also be used if the subject represents a serious threat to him/herself.

**FIGURE 8-7** Example of security officer taser affidavit training (Courtesy of HSS Inc, Denver, Colorado).

6. ECD (Electronic Control Device) use:
  - a. "ECD Displayed:" The ECD is withdrawn from the holster and visible to the subject. The subject complies without further use of the ECD.
  - b. "ECD Laser Painted:" The ECD's laser is activated and pointed in the direction of the subject and in response to the Laser printing, the subject complies without further use of the ECD.
  - c. "ECD Demonstrated:" The ECD is withdrawn from the holster, the air cartridge removed and the electrical arcing is demonstrated to the subject to attempt to gain voluntary compliance.
  - d. "ECD Deploys:" The ECD probes contact the subject's body or clothing and/or a touch stun is used to attempt to gain compliance.
  
7. Centers for Medicaid & Medicare Services (CMS) does not approve of the use of weapons by any hospital staff as a means of subduing a patient to place that patient in restraint/seclusion. If a weapon is used by security or law enforcement personnel on a person in a hospital (patient, staff, visitor) to protect people or hospital property from harm, we would expect the situation to be handled as a criminal activity and the perpetrator to be turned over local law enforcement. Again, CMS does not consider the use of weapons as safe appropriate "health care" interventions and their use is not appropriate in the application of patient restraint or initiation of seclusion.
  
8. Never use the X26 Taser near flammable liquids, fumes, or explosive environments.
  
9. Keep hands away from the front of the unit at all times unless the safety slide is in the SAFE position and the X26 Taser is deactivated.
  
10. DO NOT fire the X26 Taser near flammable liquids, fumes, or explosive environments.
  
11. No officer will playfully, maliciously, or intentionally misuse the X26 Taser in a display of power against an individual, except to counter an imminent threat. Violation of this policy will result in disciplinary action.
  
12. Probes – Biohazard:
  - a. Probes that have been deployed and strike the subject will be treated as biohazard sharps. They may be placed point down into the expended cartridge bores and secured (e.g., with latex glove(s), tape, etc.
  - b. Where ECD probe deployment is not a reasonably foreseeable issue, and where there is no indication of serious injury, probes and expended cartridges need not be routinely maintained as evidence. They shall be properly disposed of.
  - c. If the incident is non-routine, or if serious injury is alleged, then the probes and the expended cartridge(s) shall be maintained as evidence appropriately secured and marked as biohazard.
  
13. Anytime an officer discharges the X26 Taser, even if the discharge was accidental, a Security Incident Report must be written detailing the nature and reason for the discharge and the supervisor must be immediately notified.
  
14. When the X26 Taser is used against a person, the person must be evaluated by trained healthcare professionals and monitored for the individual's safety.

PRINT NAME \_\_\_\_\_ SIGNATURE \_\_\_\_\_ DATE \_\_\_\_\_

WITNESS \_\_\_\_\_ DATE \_\_\_\_\_

FIGURE 8-7 (Continued)



such as asthma or emphysema.<sup>21</sup> This potential risk is worsened if an individual or area is not properly decontaminated after a deployment of the chemical agent.

As pointed out with Tasers, CMS has underscored in its interpretive guidelines specific regulations regarding patient rights and in particular the use of weapons by any hospital staff as a means of subduing a patient in order to place that patient in restraint or seclusion—"it is not considered a safe appropriate healthcare intervention."<sup>22</sup> Chemical agents and specifically pepper spray are noted as weapons.

If the healthcare organization elects to allow chemical agents to be carried by security staff, its continued use should be based on consistent training related to when and how the agent is carried and under what circumstances it should be used.

## Batons

The nightstick, or baton, is considered by some to be an attractive alternative to firearms. As security equipment, it is not widely used. This weapon is often associated with brutality and has a more negative connotation for the public than firearms do. Another consideration is that a baton is a hindrance to officers in performing their routine duties. It constantly bangs into doorways, makes it awkward to sit, and makes it difficult to respond to emergency calls for service quickly. Those who favor the baton argue that it is a discriminating weapon that copes with the problem at hand and makes contact only with the intended person. It is difficult, however, to avoid head strikes in many cases. Paralysis or death may occur even days later as a result of subdural or bilateral hematoma.

The collapsible baton is gaining some favor and can be carried on the duty belt without the same negative perception. The small compact size of this baton eliminates many of the arguments against the use of the regular nightstick or baton. However, its use can still be perceived as undue force. For this reason, most healthcare security programs prohibit their use.

## Protective Vests

The advent of soft-bodied armor vests used by many law enforcement agencies has spawned some interest for the healthcare security industry. Today's protective vests are thin enough to be concealed under a uniform shirt. Alternatively, few healthcare security programs wear protective vests on top of their clothing. Whether they choose to conceal the protective vest depends on what type of image the healthcare security program wants to provide to the public.

A survey of 79 hospitals, all in large US cities, indicates very limited use of these protective vests. The hospitals surveyed averaged 318 beds; no hospital with fewer than 200 beds was included in the survey. Results of the survey indicated that 10% had formulated a policy on the use of protective vests. In most cases where vests are utilized, the policy provides that security officers buy their vest and that use is optional.<sup>23</sup> Healthcare organizations with employees who are authorized to carry a firearm should strongly encourage their employees to wear protective vests.

Protective vests are not just for firearm combat situations; they can also be worn to shield security officers from the harm of other weapons. In Ireland, security staff at Mercy University Hospital, a city center hospital in Cork, have taken to wearing stab-resistant vests to protect themselves against stabbings. The hospital is believed to be the first in Ireland to wear the protective vests in response to two doctors injured in a stabbing incident involving a psychiatric patient.<sup>24</sup> This follows a trend in the United Kingdom, where hospital security staff are frequently equipped with stab-proof vests, shields, and helmets to protect them against violent patients and relatives. The protective vests have improved security staff morale and contained worker's compensation costs. The UK National Health Service estimates that violence costs their hospitals around £100,000 a year in security, time off for affected staff, and legal costs.<sup>25</sup>

Security staff must remember that protective vests only provide partial protection, not absolute protection. A significant residual risk remains even if vests are worn.

## The Duty Belt

One of the most important parts of the security officer's uniform is the duty belt, on which security officers carry the equipment that must be with them at all times. At minimum, the healthcare security officer duty belt should consist of a tactical flashlight and holder, a radio and holster, and include a key keeper. If organizationally permitted, it could also include a handgun and/or Taser and holster, handcuffs, baton, or chemical spray. Some will also carry their own small notebooks and ink pen, and may also carry a cell phone. All of the equipment that is carried by the security officer on his duty belt must be evenly distributed across the belt so that it is less likely to shift or cause back strain.

Many of the items listed are not lightweight items, but heavy-duty, high-performance equipment. With few exceptions, the gear that is carried is decided by the healthcare organization, not individual judgment. Hospital security staff are advised to be prepared for any situation, but if the duty belt weighs so much that it fatigues the officer, shifts around while on patrol or responding to a critical event, or does not allow free movement it can be more of a hinder than a help. A strict policy of authorized equipment should be prepared that includes standards for how the duty belt is to be worn and what equipment can or is required to be carried.

The traditional use of leather duty belts has given ground to the use of nylon. Nylon has certain advantages over leather:

- It is fairly easy to decontaminate.
- It is durable and therefore lasts a long time.
- It is lightweight.
- It is scratch-resistant and won't stretch.
- It is cost-competitive with leather.

A subject that ties directly to the equipment used by healthcare security officers is the escalating use of force policy that every healthcare security program should have in place.

In the context of force, the security officer must be aware of how the equipment operates, a clear understanding of when it should be used and the limitations that may exist with using equipment to facilitate a patient outcome.

## Use of Force

The use of force by healthcare security officers is sometimes necessary to maintain order and safeguard staff, patients, and visitors in a healthcare environment. The security officer must occasionally use a certain amount of force, from mere presence and verbal persuasion to physical intervention, to overcome resistance and ensure compliance with hospital policy and medical care plans.

As outlined in this chapter, there are various tools and mandated limitations on the use of force in the healthcare setting. In *Garcia v. Bronx Lebanon Hospital*, 2001 WL 128893 N.E. 2d-NY, the appellate courts ruled:

*even assuming the (security officers) were justified in using force to subdue the patient because of his own inappropriate conduct; the court found an issue remained as to whether the degree of force used was reasonable under the circumstances. Even if the use of force was justified, the security (officers) could lawfully use only that amount of force necessary to control the patient, no more!*<sup>26</sup>

Every healthcare facility should develop a use of force policy that include the identification of situations, both clinical and non-clinical, in which security officers are permitted to use force. IAHSS has developed a guideline which outlines the basic aspects of such a plan.

### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.05

#### **Security Officer Use of Physical Force**

**STATEMENT:** Healthcare facilities (HCFs) will develop policies and procedures that include the identification of situations, both clinical and non-clinical, in which security officers are permitted to use force. The amount of force to be used will be that which is objectively reasonable and takes into account the totality of the circumstances.

#### **INTENT:**

- a. Use of force is defined as any force beyond a guiding touch. All government requirements, accreditation, and regulatory (i.e., CMS) guidelines should be consulted in the development of this policy. Appropriate force used to prevent attack, illegal activity, or to detain a person may be justified under the above requirements.

- b. The policy should contain a use of force educational element such as a matrix or a continuum. This element would provide guidance to the security officer detailing the appropriate response to the level of resistance being encountered.
- c. The HCF will determine if weapons are to be carried by security personnel. This decision should be based on a security assessment of the individual facility, local crime statistics, and other factors as deemed necessary and will help determine what specific weapons, if any, are authorized.
- d. The HCF will determine what restraints, if any, will be carried and under what circumstances they may be used. Also, as part of the security assessment this decision would be based on a calculated need as indicated by past experience.
- e. Terms such as “least amount of force” or “only necessary force” should be avoided because of being subject to interpretation. The recommended terms “objectively reasonable,” the “totality of the circumstances,” and “reasonably appears necessary” have been court tested and are preferred.
- f. HCF will insure initial and ongoing training of policies and procedures to include the physical skills training necessary to demonstrate competency in the use of force. This training documentation will be maintained as part of the security officer’s training record.
- g. All incidents involving the use of force by security officers will be documented. A special use of force form may be maintained with the original report of the incident.

**REFERENCES/GENERAL INFORMATION:**

- *Graham v. Conner* 490 U.S. 386 104 L. Ed. 2d 443, 190 S. Ct. 1865 (1989)
- International Association of Chiefs of Police National Law Enforcement Policy Center USE OF FORCE Model Policy, August 2001
- Healthcare Security: Basic Industry Guidelines. Glendale Heights, IL: International Association for Healthcare Security and Safety
- IAHS Guideline: 02:04, “Security Role in Patient Management”
- IAHS Guideline: 03:01, “Security Officer Training”
- Journal of Healthcare Protection Management, IAHS 2007 Volume 22, No. 2, Page 155, Use of Force in Private Security: A Primer.

**Approved:** November 2007

## Training

Deciding on the proper equipment to be used by security officers is an important first step, but it does not end there. The proper use of each item is essential. Initial officer training must be supplemented with periodic retraining. Equipping the officer with non-essential items needlessly increases the training time and the resulting program cost.

## Security Operations Manual

The security operations manual brings together the security policy, standards, and general procedures. This manual should not be confused with the employee handbook,

which basically contains the personnel policies of the organization. It is intended to furnish security officers with the information needed to perform their job effectively. The content of this manual varies from organization to organization. The typical manual includes the following general information:

1. Purpose and scope of the healthcare organization.
  - Table of organization
  - Key personnel (possibly with pictures)
  - Plot plans
2. Purpose and scope of the security program
  - Organizational chart
  - Position descriptions (brief narratives)
  - General and special orders
  - Training program
3. Security records and reports.
  - Types
  - Intended utilization
  - Distribution
4. General security information.
  - Use and care of equipment
  - Fire and safety information

The style, format, and content of the security manual are determined by individual program preference. A loose-leaf notebook is one style that permits the easy insertion of revised information or additional material. A powerful new piece of technology is to store the security manual electronically and make it available to the security officer via personal digital assistant (PDA). Carried on the duty belt, and typically small enough to fit in the palm of the hand, these pocket PC have proven to be invaluable time savers. Communications can be automated and provide security officers with updated checklists and instructions for their day-to-day activities and patrol. Also used for real-time incident notification, this technology can be a valuable resource to security officers who need to view a CCTV image or refer to their specific response during a hospital disaster.

## References

1. Lutz, S. (1990). Border hospital's guard garb ripped (Note: Best information provided). *Modern healthcare* (December 17), 8.
2. Weonik, R. (2008, January 21). *Securing our hospitals: GE security and IAHS&S healthcare benchmarking study*. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
3. Potter, A. N. (2006). *Considerations when arming hospital security officers*. Retrieved March 31, 2009, from <http://www.iahss.org/Ref-Materials/Potter-Paper/Contents.htm>. Pg. 8.

4. Potter, A. N. (2006). Considerations when arming hospital security officers. Retrieved March 31, 2009, from <http://www.iahss.org/Ref-Materials/Potter-Paper/Contents.htm>. Pg. 8.
5. Thompson, B. (2005, March 3). *Hospital security and personnel safety concerns*. Presented at Henry Ford Medical Center.
6. 6 requirements your radios should address. (2009, April 8). *Campus Safety Magazine*. Retrieved April 9, 2009 from <http://www.campussafetymagazine.com/MotoEpromo>.
7. Department of Health and Human Services. (2006, December 8). *Hospital conditions of participation: patient rights*. Retrieved June 16, 2008, from <http://www.cms.hhs.gov/CFCsAndCoPs/downloads/finalpatientrightsrule.pdf>, §482.13(e).
8. McCauley, D. (1996). Gasping for breath (Note: best information provided). *Police*, 5(July), 56–58.
9. Roberts, J. R. (2007, September). The acutely agitated patient: Fatalities and physiology. *Emergency Medicine News*. Retrieved April 4, 2009, from <http://www.em-news.com/pt/re/emmednews/fulltext.00132981-200709000-00029.htm>.
10. Confronting and dealing with problems of latex-based products. (1997). *Hospital Security and Safety Management*, 17(11), 5–7.
11. Centers for Disease Control. *Guidance for the selection and use of personal protective equipment (PPE) in healthcare settings*. Retrieved April 4, 2009, from <http://www.cdc.gov/ncidod/dhqp/pdf/ppe/PPEslides6-29-04.pdf>.
12. Taser International. (2008, September 9). *Instructor certification course, version 14.2*. Retrieved June 17, 2009, from <http://www.taser.com/training/Documents/Training%20Bulletin%202014.2-01.pdf>. Pg. 13.
13. Taser International. (2008, September 9). *Instructor certification course, version 14.2*. Retrieved June 17, 2009, from <http://www.taser.com/training/Documents/Training%20Bulletin%202014.2-01.pdf>. Pg. 8.
14. Weonik, R. (2008, January 20). *Securing our hospitals: GE security and IAHS healthcare benchmarking study*. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
15. St. John's officers to stop carrying tasers. (2008, September 9). *Springfield News-Leader*. Retrieved September 9, 2008, from <http://www.news-leader.com/article/20090405/NEWS01/904051542/1007/NEWS01>. (Note: best information provided).
16. Hospitals debate stun gun use in security departments. (2004, July 26). *Environment of Care Leader*, 9 (14), 7. (Note: best information provided).
17. Stanbrook, M. B. (2008, May 20). Tasers in medicine: an irreverent call for proposals. *Canadian Medical Association Journal*, 178 (11). Retrieved April 3, 2009, from <http://www.cmaj.ca/content/vol178/issue11/#EDITORIAL>.
18. Bozeman, W. P., Hauda, W. E., Heck, J. J., Graham, D. D., Jr., Martin, B. P., & Winslow, J. E. (2009). Safety and injury profile of conducted electrical weapons used by law enforcement officers against criminal suspects. *Annals of Emergency Medicine*, 53(4), 480–489.
19. Strote, J., & Hutson, H. R. (2006). Taser use in restraint-related deaths. *Prehospital Emergency Care*, 10(4), 447–450.
20. Stefan, S. (2006). *Emergency department treatment of the psychiatric patient: Policy issues and legal requirements*. New York: Oxford University Press, p. 37.
21. Stefan, S. (2006). *Emergency department treatment of the psychiatric patient: Policy issues and legal requirements*. New York: Oxford University Press, p. 37.

22. Department of Health and Human Services. (2006, December 8). *Hospital conditions of participation: patient rights*. Retrieved June 16, 2008, from <http://www.cms.hhs.gov/CFCsAndCoPs/downloads/finalpatientrightsrule.pdf>, §482.13(e), 96.
23. Bakos, B. (1993, July). Utilization of bullet-resistant vests in healthcare facilities. Unpublished research study, 1–11.
24. O'Regan, E. (2008, September 10). *Security staff don stab vests as hospital knife crime risks rise*. Retrieved June 18, 2009, from <http://www.independent.ie/national-news/security-staff--don-stab-vests-as-hospital-knife-crime-risks-rise-1472815.html>.
25. Hospital staff to wear stab-proof vests as violent patients on the increase. (2007, June 3). *Evening Standard*. Retrieved June 18, 2009, from <http://www.thisislondon.co.uk/news/article-23387896-details/Hospital+staff+to+wear+stab-proof+vests+as+violent+patients+on+the+increase/article.do>.
26. Tammelleo, A. D. (2001, October 1). NY: hospital security guards subdue patient: Was more than minimum necessary force used? *Hospital Law's Regan Report*. Retrieved April 10, 2009, from <http://www.allbusiness.com/professional-scientific-technical-services/legal-services/823589-1.html>.

# Training and Development

The need for adequate training of security personnel is vigorously espoused by management and line personnel alike. It is a subject that gets constant attention at security meetings and seminars; is probed during security reviews and audits; gets considerable space in magazines, newsletters, and journals; is sanctioned by consumers and providers; and is the basis of many lawsuits. However, this almost insatiable quest for proper training appears to break down at the design and implementation stage in many healthcare security programs. One of the most critical challenges—and one of the most basic responsibilities—of the security administrator is to provide the means for each person in the security department to achieve the competency level required to perform the function as stated in the job description. A good security officer training program requires a master plan that addresses everything from identifying needs for the newly hired security officer to ongoing education and development activities established for seasoned security staff and security department leadership positions. It cannot be understated how important the verification of skill levels and documentation are to the successful healthcare security training plan. The proper training of the security staff is a direct reflection on the security administrator's commitment to quality and customer service.

Certain basic elements or steps in the training process must be addressed and tailored to each healthcare organization. There should be a combination of generic healthcare security training with training specific to the organization. An example of this blending is that of report preparation. The basics of how to collect information and prepare a report are somewhat the same for all organizations. However, the types of reports and methods utilized to accomplish the completion of a report are specific to each organization. For example, the International Association for Healthcare Security and Safety (IAHSS) basic training manual for healthcare security officers provides a generic approach to healthcare security officer training as a foundation to be supplemented by training relative to specific facility security program tasks. Other important points to remember include:

- Job descriptions should provide the basic source of job task analysis to pinpoint specific skill levels required. Policies and procedures of the entire organization, not just security policy and procedure, will further identify skill-level needs.
- Determine performance objectives, which in turn will be utilized to develop the knowledge required of the security officer to competently complete the tasks identified. The objective is what the trainee must know. Without clearly stated objectives, there can be no competency-based training.



- Develop clear measurement standards in order to determine whether the performance objectives of the training endeavor have been accomplished. The objective is to insure that everyone understands what is expected of them and what constitutes below average, average, and excellent performance.<sup>1</sup>
- Verification of whether there was a sufficient transfer of information from instruction to actual situation performance.
- Develop dynamic (up-to-date) curriculum and select training methods and materials.

The Wackenhut Training Institute, in Coral Gables, FL, has taken an emerging adult learning model as its approach to training. This model is known as *andragogy*, a term developed by Malcome Knowles, a widely known adult educator. Andragogy embraces the following four tenets of adult education:

- Adults want to be self-directed as opposed to instructor-directed (goal-oriented).
- Adults bring unique life experiences to the learning process (respect for their experience is a must).
- Adult learning is linked to what adults consider relevant (how will the lesson be useful to them on the job).
- Adults want an immediate application of learned knowledge (hands-on component).

This model is a very practical approach to healthcare security training; however, it is more difficult for both student and instructor. Students must stop thinking of themselves as students and realize they are adult learners with a responsibility in the training process. Likewise, instructors must think of themselves as facilitators of adult learning.<sup>2</sup> As with all learners, adults want to be shown respect.

Litigation has been a powerful driving force in the increase in healthcare security officer training. Claims that healthcare organizations have failed to provide necessary training are used with much success in lawsuits, especially those involving weapons, physical force, false arrests, and civil rights issues. The responsibility for the adequate training of security staff rests squarely on the organization.

Meanwhile, it seems that there are never enough security officers to really get the job done, and we often think more is better. The need for better-trained officers is expressed far less frequently. Ironically, although a trained security officer can be at least twice as productive as a well-intentioned untrained officer, it is usually easier to obtain money for an extra position than for additional training. The number of security personnel is often mistakenly used to determine the level of protection, regardless of the training required of or provided for the position.

In HCFs, extensive training is apparent in almost all departments. The medical care arena focuses on training and continuous in-service education at almost every level. Dietitians, medical technicians, health information management clerks, nursing assistants, registered nurses, and environmental services personnel undergo training in one form or another. Our demand for the highest quality healthcare requires ongoing education for healthcare providers of every description. Security should be no exception.

One of the basic hurdles that influence training programs is security officer turnover. An organized security officer training program can reduce turnover as it improves morale and offers an avenue for personal growth. Well-trained officers who know they are competent exhibit a higher level of job interest and job satisfaction than others do. Proprietary security programs, except very large ones, simply cannot provide extensive formal instruction for one or two officers. On the other hand, in-house programs generally have more funds for training than do contract security agencies, which are limited to providing services at a fixed cost.

## Training Concepts

The term *training* includes preassignment training and, more importantly, continuous training throughout the career of the security staff member. Security officers are often classified as “trained” or “not trained.” This concept should yield to the idea of level of training.

There is a difference between training and education. Christopher Hertig, an instructor at York College of Pennsylvania, makes such a distinction. He states, “Training is an intensive process whereby an employee’s job behavior is modified. Training prepares and enables a person to perform job tasks at a greater level of efficiency. Education is knowledge about something. It’s the understanding of concepts and principles that enable a person to grow professionally; knowledge that provides one with an appreciation of various job functions. Education teaches the ‘whys’; training teaches the ‘hows.’”<sup>3</sup>

Training must be relevant. As simple and basic as this consideration seems, some training is given merely to fill the allotted time or because an instructor is available. An often neglected area of training is the operational aspect of the healthcare delivery system. Security officers should learn how various departments and sections of the healthcare system operate to understand better what they are protecting and their role in the delivery of quality patient care. The better officers understand the operations, the formal and informal hierarchy, and the history, objectives, and goals of the organization, the better equipped they will be to carry out their responsibilities.

### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #03.01

#### **Security Officer Training**

**STATEMENT:** Healthcare facilities (HCFs) will ensure that any individual performing security services are trained to meet local, state or federal standard for security officer training and healthcare security industry standard practices.

#### **INTENT:**

- a. Training should include a method to verify that the training received resulted in an acceptable level of competency for each person trained.

- b. Retraining, especially for high-liability subjects such as weapons training, workplace violence prevention and response skills, and management of physical aggression should be conducted at least annually.
- c. Training records for each individual should be maintained by the HCF according to the HCF record retention policy.
- d. Training records should include the subject matter, time and duration of training, and instructor's name and affiliation.
- e. HCFs are encouraged to achieve and maintain certification levels developed by IAHS or similar.
- f. If a state or local entity with jurisdiction proscribes mandatory training for contract officers, but not proprietary officers, the HCF should at least provide an equivalent level of training for proprietary officers.

**REFERENCES/GENERAL INFORMATION:**

- IAHS Security Officer Training Manuals and Study Guides.

**Approved:** January 2006

**Last Revised:** October 2008

## Types of Training

Considerable dialogue and printed materials are available relative to the type and content of training appropriate for healthcare security officers. There are five fundamental types of training the healthcare security program must give significant consideration: new security officer training, IAHS Progressive Certification, specialized program training, elective training, and security leadership development activities.

The new security officer training is the basic security training applicable to virtually every security officer and provides the foundation of knowledge that allows for a successful career. Beyond the healthcare organization's orientation program for new employees, new security officers should be exposed to a mixture of instructor-led training and task-specific on-the-job training (OJT). The IAHS Progressive Certification training programs described in this text are considered basic areas of training which, when supplemented by specialized training, can significantly enhance security officer performance. Specialized training takes into consideration the function and responsibility of the officer in a specific organizational setting. Like the new security officer training, both IAHS certification and specialized training should be considered a fundamental part of the organization-mandated officer training.

Elective training involves training or education that is generally not mandatory. It is usually taken by the officer who has a personal interest or personal objective for participating in specific self-improvement activities. These training activities are generally pursued on the individual's own time.

Leadership development activities cannot be lost in the healthcare security training program. They can increase the effectiveness of the supervisors, managers, and directors involved in the healthcare security program and be the source for driving higher levels of

both patient and employee satisfaction. Helping security leaders at various levels develop the skills and knowledge they need to succeed in their leadership positions can make the organization a better place to work and help the protection program retain its most critical asset—their employees. Many healthcare organizations have seen that investment in the development of its security leaders has a measurable return on investment (ROI) as it helps reduce costs in the areas of turnover and employer-practice and inadequate security liability.

## New Security Officer Training

Professional security officer training is a combination of protection, customer service, and public relations. The security officer reflects the customer-service attitude and security posture of the HCF. Proper training of newly hired security officers can produce the ROI in terms of attaining the highest level of security and safety. Each new security employee should receive a series of training modules designed to provide security-specific education and healthcare-specific training in an efficient and verifiable manner. The training of new security personnel should be to a standard of performance and not just to the time allotted.

The amount and quality of preservice training for the new security officer is critical to the success of the officer and to the delivery of high-quality services. Unfortunately, much preservice training consists of on-the-job instruction of a new officer by another officer. The disadvantages of this method are obvious. New officers become only as proficient as their teachers, and they often learn the wrong way from the beginning. On the other hand, a formal 40-, 60-, or 80-hour instructor-led course is cost-prohibitive and rarely conducted for one or two newly hired officers.

This dilemma illustrates the difficulty of outlining a preservice training program where there are many variables, such as the size of the security force and the availability of resources. The approach for a security force of three or four members must inevitably differ from that of a security department of 30 or more officers.

## On-the-Job Training

Although OJT has its shortcomings, it is necessary for providing officers with hands-on experience. There is no substitute for demonstrating the tasks that must be completed. A failing of many OJT programs is the lack of a formulated structure. The OJT trainer should use a predetermined checklist when providing instruction. [Figure 9-1](#) is an example of an OJT preservice training checklist used at Hanover Hospital in Hanover, PA. Both the OJT trainer and the trainee sign the checklist after the instruction is completed, and this checklist becomes part of the officer's permanent training record. This preservice training should be followed up by some form of competency testing.

## Critical Task-Focused Training

Training to a time period versus an established standard coupled with the absence of a competency verification philosophy and defined post-orders creates risk of liability for inadequate training, supervision, and significantly increases training-related expenses.

**Hanover Hospital Safety and Security  
On the Job Training**

ON THE JOB TRAINING CHECKLIST	TRAINEE INITIAL	TRAINER INITIAL
<b>1. Introduction</b>		
Site Location		
Hanover Hospital Table of Organization		
Hospital Department Locations		
Hospital Floor Plans		
<b>2. Security Officer Job Description</b>		
Security Officer Job Description		
Security Officer Job Performance Standard		
<b>3. Security Department Rules and Regulations</b>		
Chain of Command		
Department Rules and Regulations		
Company Rules and Regulations		
Officer Attendance and Scheduling		
Uniform Requirements and Dress Code		
Reporting For and Off Duty		
<b>4. Security Post Procedures</b>		
Post 1 Procedures		
Foot Patrol Procedures		
Emergency Phone Numbers		
Emergency Contact Information		
Primary Duties and Responsibilities		
Daily Activity and Incident Reports		
Specific Duties and Responsibilities		
Specific Post Assignment Duties and Responsibilities		
<b>5. Access Control</b>		
After Hour Visitation		
Employee Identification Badges		
Contractor Identification Badges		
Shipping and Receiving		
Deliveries During Business Hours		
Deliveries After Business Hours		
Removal of Hospital Property and Equipment		
Card Access System		
Security Sensitive Areas Policy		
Infant Abduction System		
Delayed Egress		
Emergency Lockdown		
<b>6. Patrol Procedures</b>		
Pro-Active		
Patrol Tour Points		
Issuing Parking Notices		
Responding to Off-Site Facilities Alarms/Assignments		
Parking Policy		

**FIGURE 9-1** A sample on-the-job training checklist for a healthcare security officer (Courtesy of Hanover Hospital, Hanover, Pennsylvania).

Hanover Hospital Safety and Security  
On the Job Training

ON THE JOB TRAINING CHECKLIST	TRAINEE INITIAL	TRAINER INITIAL
7. Emergency Response Procedures		
Code Red		
Evacuation (4 Methods)		
Code Pink		
Code Green – Primary Officer		
Code Green – Back Up Officer		
Code 9		
Code Yellow		
Code Purple		
Code Brown		
Code Silver		
Code Orange		
Mechanical Problems		
Electrical Problems		
Elevator Problems		
Water Leak		
Severe Weather		
Criminal Activity		
Media Relations		
Interim Security Measures Policy		
Emergency Management Plan		
Radiation Alarms		
8. Miscellaneous Procedures		
Key Control Policy		
Lost and Found Policy		
Patient Valuables Policy		
Infant Abandonment Policy		
Restraint Policy		
Traffic Control		
Radio Usage and Communication		
Employee Escort Service		
Vehicle Assistance		
Telephone Usage		
Forensic Patients Procedures		
9. Video Training		
Video #1 MRI Magnet Safety: The Invisible Force		
Video #2 Fire Response and Control for Hospital Security		
Video #4 Report Writing for Hospital Security		
Video #5 Fire Safety Within the Hospital Setting		
Video #7 Disaster Response “Security’s Role”		
Video #8 Chemical Hazards in Healthcare		
Video #9 Worker’s Enemy #1: Back Sprains		
Video #10 Role of a Hospital Security Officer		

FIGURE 9-1 (Continued)

**Hanover Hospital Safety and Security  
On the Job Training**

ON THE JOB TRAINING CHECKLIST	TRAINEE INITIAL	TRAINER INITIAL
<b>10. Required Training</b>		
Nonviolent Crisis Intervention (CPI)		
CPR		
Wheelchair Safety and Operations		
Emergency Response Team Training		
Decon PAPRs		
Decon and Seclusion Rooms		
Clinical PAPRs		
Computer Operations/Procedures		
ProWatch Software		
IRIMS Software		
Act-Track Dispatch Log Software		
LZ-46 Driver Training and Inspections		
Code — 40		
Signal-36		
Company Car Operation		
<b>11. Testing of System</b>		
Infant Abduction System – Weekly		
State Radio – Weekly		
Blue Light Call Boxes – Weekly		
In-House Panic Alarms		
Off-Site Panic Alarms – Quarterly		
Brokey System		

FIGURE 9-1 (Continued)

**Hanover Hospital Safety and Security  
On the Job Training**

**ON THE JOB TRAINING RECORD**

\_\_\_\_\_ Trainee Name \_\_\_\_\_ Trainee Signature

\_\_\_\_\_ Hire Date \_\_\_\_\_ On The Job Training Completion Date

-----  
I, \_\_\_\_\_ & \_\_\_\_\_, conducted the training for this officer and he/she has satisfactorily completed all the Job Training items through direct involvement, supervision, and observation.

\_\_\_\_\_ Trainer Signature \_\_\_\_\_ Trainer Signature

Comments:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Strengths and Weaknesses:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**FIGURE 9-1** (Continued)

Time to train is irrelevant. There are a number of state statutes that mandate how many contact hours should be provided for security staff training. Most healthcare security professionals agree competency is a better indicator of future success. Many healthcare protection programs have determined that the amount of training time provided is not a good judge of an individual security officer’s aptitude to perform the function of protecting a healing environment—their demonstrated competency is a preferred indicator.

Competency-based training has become a buzzword coming from TJC and the comments made during their on-site survey. TJC surveyors are no longer solely interested in



the documented “check the box” training. The surveyors are asking security officers to demonstrate, or at minimum, describe, their responsibility (competency). An example of this trend is found at a northern California hospital. Two hospital security officers who had been on the job for 6 months were asked detailed questions by a TJC administrative surveyor regarding their specific role and responsibilities in a community-wide mass casualty disaster. Questions asked ranged from traffic control to their individual role in the decontamination process. After the exchange, each security officer was commended by the TJC surveyor for his/her knowledge and understanding of his/her role in the disaster. The personnel jacket of each security officer was reviewed later, but specific training documentation was never requested. This example is one of hundreds where TJC surveyors have transitioned their focused questioning from just a basic exposure to that of competency.

### *Competency Verification*

Competency verification starts with security leadership. Security leaders, field training officers, or anyone with the responsibility for training security staff must answer a simple question—“How do I know that my staff is competent?” The process begins by identifying those tasks most critical to the healthcare security officer. A training plan is then developed for each task by creating a job list that provides systematic instructions for how each “task” is accomplished. [Figure 9-2](#) demonstrates a sample competency format used for a basic task carried out by a healthcare security officer.

**Sample Critical Task Format**

<b>FACILITY:</b>		<b>UPDATE:</b> 05/01/2009
<b>TASK:</b> Very Important Patient		<b>LEARN SEQ:</b>
<b>ELEM</b>	<b>ELEMENT DESCRIPTION</b>	<b>COMP</b>
1	Able to define a VIP	Yes No
2	Do not make statements to media on behalf of the hospital or HSS	Yes No
3	Refer media members to official spokesperson described in hospital policy	Yes No
4	Generally restrict media members, movement throughout the facility	Yes No
5	Notify hospital administration, Risk Management, and public safety agencies as directed	Yes No
6	When a security officer is posted, assign a patient room away from elevators and fire stairwells or exits; when a security officer is not posted, assign a room with good visibility from the nursing station	Yes No
7	Remove the patient name from switchboard, Front Desk, and census reports, and replace with an alias for the actual patient	Yes No
8	Maintain the patient's chart in the patient's room	Yes No
9	Brief the nursing unit staff of general information or specific action items required of hospital staff	Yes No
10	Determine if any person may visit	Yes No
11	Obtain the name and telephone number of persons coordinating security for the VIP, persons who can answer questions, and persons to contact in an emergency	Yes No
12	Write SIR, category PATIENT ASSISTANCE, _____	Yes No
<b>TASK</b>	The officer can perform each of the elements	Yes No

**FIGURE 9-2** A sample competency format used for a basic task performed by a healthcare security officer.

The underlying purpose of this system of learning is identifying information and skills needed by security staff to meet job performance requirements. A security officer who can demonstrate, explain, and define the role and responsibility can perform the following:

- Demonstrate: *How the task is completed.*
- Explain: *Why the task is completed.*
- Define: *The importance of the task.*

Task training should present information in a goal and learning objective concept, so that information can be absorbed and retained. Task training information, when presented in a prioritized sequence, provides a systematic approach to identify learning weaknesses and measure learning goals. Some healthcare security programs break down the task list into two sections: (1) the mission-essential competencies that must be known prior to donning a uniform and (2) those that must be known within a predefined period of time, typically 60–90 days.

The foundation of the competency inventory is developed from security program documents such as the department post orders, policy and procedures, and other protocols, in addition to the Hospital Policy Manual and Hospital Emergency Preparedness Manuals. A sample of how a healthcare organization can sequence the learning of a security officer task inventory is shown in [Figure 9-3](#).

A key component for the critical task-focused training program is the verification of knowledge by a supervisor or training officer. The officer must confirm their knowledge by demonstrating and/or describing their comprehension of each critical task to a person in a responsible charge position. Thus, separating the responsibility of who trains the security officer and who verifies competency is ideal.

## Key Training Topics for the New Security Officer

Professional security officers must be prepared to subdue a mentally disturbed patient, apprehend a thief, comfort a distraught mother, escort a lost visitor, and perform any number of other tasks at any time, anywhere in the facilities they serve. To prepare security officers for this demanding job, the healthcare organization must invest in the development of a comprehensive, industry-specific, multistep training program focused on protection, public relations, and customer service. Training is not a one-time event. From the time hired and throughout their careers, security officers must continue training to learn, improve, and further develop their professional skills.

### *Security Role in Patient Care/Aggression Management*

A primary role of security staff in the healthcare environment is to assist care providers in managing at-risk patient behavior. Healthcare security officers can expect to be called

**New Employee Training Program  
Critical Task Learning Prioritization/Learning Sequence**

OFFICER \_\_\_\_\_ Hire Date \_\_\_\_\_

PHASE	TASK #	TASK	COMP	PHASE	TASK #	TASK	COMP
<b>ORIENTATION FIRST WEEK</b>	O-1	Security Documentation	Y N	<b>PHASE I FIRST 2 WEEKS</b>	PH I-1	Patient Searches	Y N
	O-2	Radio Communications	Y N		PH I-2	Patient Restraint Application	Y N
	O-3	Courteous Enforcement	Y N		PH I-3	Patient Elopement/Response	Y N
	O-4	Facility Locations	Y N		PH I-4	Patient Valuables Process	Y N
	O-5	Codes	Y N		PH I-5	Missing Patient	Y N
	O-6	Patient Assistance	Y N		PH I-6	Defensive Driving	Y N
	O-7	Security/Fire Alarm Response	Y N		PH I-7	Security Patrol Vehicle Use	Y N
	O-8	PPE	Y N		PH I-8	Facility Patrols	Y N
	O-9	Aggression Management	Y N		PH I-9	Security Alarm Locations	Y N
	O-10	Security Key Ring/Control	Y N		PH I-10	Report Writing	Y N
	O-11	Use of Force	Y N		PH I-11	Trauma/Core 0 Team	Y N
	Internal	Hosp. New Emp. Orientation	Y N		PH I-12	After Hours Access Control	Y N
New Officers must complete Orientation Phase and have Security Manager approval to begin Phase I				New Officers must complete Phase I and have Security Manager approval to begin Phase II			
Security Manager _____ Date _____				Security Manager _____ Date _____			

PHASE	TASK #	TASK	COMP	PHASE	TASK #	TASK	COMP
<b>PHASE II FIRST 30 DAYS</b>	PHII-1	Missing/Found Property	Y N	<b>PHASE III FIRST 60 DAYS</b>	PHIII-1	Internal Disaster Response	Y N
	PHII-2	Forensic Patient	Y N		PHIII-2	External Disaster Response	Y N
	PHII-3	Helicopter Assist	Y N		PHIII-3	Bomb Threat Response	Y N
	PHII-4	Morgue Duties	Y N		PHIII-4	Serious Incident Notification	Y N
	PHII-5	Discovered Fire Response	Y N		PHIII-5	Hostage Situation	Y N
	PHII-6	Injured Person Assist	Y N		PHIII-6	CCTV Locations	Y N
	PHII-7	Civil Disturbance	Y N		PHIII-7	Very Important Patient	Y N
	PHII-8	Vehicle Battery Jump	Y N		PHIII-8	Snow Removal	Y N
	PHII-9	Vehicle Tire Change	Y N		PHIII-9	DECON Suit Training	Y N
	PHII-10	Infant/Pediatric Abduction	Y N		PHIII-10	Visitor Management	Y N
	PHII-11	Detox Transport	Y N		PHIII-11	Package Inspection	Y N
	PHII-12	Door Unlock Requests	Y N		PHIII-12	Non-Solicitation Policy	Y N
	PHII-13	Personal Escort	Y N		PHIII-13	Arrest, Search & Seizure	Y N
New Officers must complete Phase II and have Security Manager approval to begin Phase III				New Officers must complete Phase III and have Security Manager approval to begin Phase IV			
Program Security Manager _____ Date _____				Security Manager _____ Date _____			

FIGURE 9-3 A sample sequenced and prioritized critical task list for a healthcare security program.

upon to de-escalate and manage aggressive or violent behavior. Every healthcare security program should have a training offering to guide officer response and behavior in a manner that reflects the HCF's philosophy of patient care. Focusing on verbal de-escalation and voluntary compliance, the program should be designed to teach security staff

members to successfully control aggression and other verbal or physically inappropriate actions of others in a medical care environment.

Sensitivity training is also important and often combined with the de-escalation-type training. Sensitivity training gives security officers alternatives to the use of force when dealing with people. It takes a humanistic—or sympathetic—approach to solving people’s problems and tries to provide insight into why people behave the way they do.

Some healthcare programs develop and provide their own training programs to deal with disruptive behavior, while others utilize an outside source for this training. [Table 9-1](#) identifies specialized organizations that provide aggression management training for security and healthcare staff.

Every security officer should complete this training and demonstrate competence in identified physical maneuvers early in his/her career—ideally before ever donning a uniform. Ideally, the healthcare protection program offers and requires annual refresher training and periodically audits individual officer’s ability to perform both the physical control and escape maneuvers.

### *Use of Force*

As identified in *Chapter 8, Security Staff Attire and Equipment*, every HCF should develop a use-of-force policy that includes the identification of situations, both clinical and non-clinical, in which security officers are permitted to use force. The new officer must be trained on the use-of-force policy upon hire, and be provided specific training on each item of the equipment they carry.

Each item of the equipment should be provided its own segment of training. The student should be required to demonstrate competency of classroom material presented and a high level of proficiency with the equipment. For example, an officer who carries handcuffs should be required to demonstrate proficiency handling and applying the device in addition to having a clear understanding of when this tool may be used and under what circumstances. This approach should be used with all equipment carried that falls within the healthcare organizations use-of-force continuum: zip ties, chemical agents, batons,

**Table 9-1** Aggression Management Training Programs for Security and Healthcare Staff

Available Aggression Management Training Programs	
Techniques for Effective Aggression Management (TEAM)	<a href="http://www.hss-us.com">www.hss-us.com</a>
Crisis Prevention Institute (CPI)	<a href="http://www.crisisprevention.com">www.crisisprevention.com</a>
Management of Aggressive Behavior (MOAB)	<a href="http://www.personalprotectiontraining.com">www.personalprotectiontraining.com</a>
The Mandt System	<a href="http://www.mandtsystem.com">www.mandtsystem.com</a>
Verbal Judo Institute	<a href="http://www.verbaljudo.com">www.verbaljudo.com</a>
Professional Education Services, Inc. (PES)	<a href="http://www.pesinc.net">www.pesinc.net</a>
Handle With Care	<a href="http://www.handlewithcare.com">www.handlewithcare.com</a>

electronic control devices, and firearms. The training should meet all applicable state-mandated and industry-recognized standards and include periodic refreshers.

### *Restraint Training*

Since the last publication of this text, CMS has reversed their position on security staff being able to apply medical restraints on a patient. Gone are the days of “*observe and report*” with the security officer’s primary responsibility to stand by while clinical staff apply restraints. Today, security staff are permitted to apply restraints and are often a critical team member in this patient care process. CMS recognizes that security staff involvement can cause less harm and often less pain to the patient. The basic requirement is that if a security officer is involved in the application of restraints, he/she has to be trained and demonstrate competency in the safe application and use of restraints.<sup>4</sup>

The frequency in which restraint training is offered by the HCF can often reduce the ability of the security department to render this basic function. The application of a restraint is a clinical procedure, and training is typically provided by clinical staff. Many healthcare organizations schedule the training in 6-month increments and attrition does not occur that routinely. As a result, the security officer is either not trained to hospital and CMS standards before applying restraints or is not an available resource when a situation arises that calls for medical restraints to be applied. Neither situation is enviable. To overcome this problem, many healthcare security administrators have coordinated with the resident restraint educator to train an internal security department employee as a trainer for this critical task.

The new security officer must be provided specific training and patient-centered guidelines for this specific technique for managing at-risk behavior. A “least restrictive alternative”<sup>5</sup> approach must be used. By clearly defining individual staff responsibilities and promoting patient and staff safety, these practices can reduce related worker's compensation expense and liability exposure for the HCF.

### *Report Writing*

A hospital security officer in the course of his or her duties will encounter numerous events or incidents that require the passing of factual information to others. Of all the security officer’s duties, the ability to write an accurate, clear, concise, and impartial security incident report is one of the most vital.

Security personnel must receive training in effective report writing early in their career. This training should include how to interview and obtain data, how to record information properly, as well as the rationale for this process.

New security officer training should focus on how to write a security incident report. Many organizations require the completion of sample reports based on the facts gathered from actual events. Training can also cover how the written security incident report is an official document and a reflection of the officer, the security department, and the healthcare organization as a whole. It is important for the new officer to understand that the report is frequently reviewed by others such as facility administration, insurance companies, law

enforcement, and the courts. Further discussion on the filing and completion of a security incident report is covered in *Chapter 10, Deployment and Patrol Activities*, and *Chapter 11, Program Documentation*.

### *Customer Service and Security*

Healthcare security officers who perform their job correctly spend more than 50% of their time providing general services. This is a key element of a successful security program.

As ambassadors for the organizations and the constituents served, the security officers must understand the rules of courteous enforcement and public relations. The long-term success of every healthcare security program is rooted in its evolution as a customer-service focused protection department.

Many healthcare organizations have incorporated the RATER model to improve and deliver customer service. Invented by Leonard Berry, this model identified five quality customer-service dimensions found to be relevant for the healthcare protection program and its ability to deliver “above and beyond” customer service. In examining the customer-service training provided to new security officers, the healthcare protection professional should review:

- *Reliability*: Ability of the security officers to perform their service dependably and accurately.
- *Assurance*: Knowledge and courtesy of the security officers and their ability to inspire trust and confidence in others.
- *Tangibility*: Appearance and image of the security officer; how they care for equipment; and their ability to communicate verbally and in writing.
- *Empathy*: Building the security officer’s understanding of the nature of the healthcare environment and delivery system coupled with a caring attitude.
- *Responsiveness*: Willingness of the security officer to help customers, provide prompt service, and solve problems.

More than just security, security staff members are ambassadors for the organization they serve. The image, actions, and interactions with patients, visitors, and staff the healthcare security officer has should leave a positive feeling about the hospital and the security program. The initial training provided to new security officers must reinforce this message.

### *Patrol Techniques*

The security patrol is the most common activity performed by the healthcare security officer. Patrolling officers have a unique opportunity to provide a positive service to the staff, visitors, and patients of the organization. But more than just “walking around,” the security officer must be trained to be “systematically unsystematic” to routinely change his/her patrol coverage. The new officer must learn to that while on patrol, the officer is looking for people in need of assistance or dangerous situations and how to use his/her senses (sight, hearing, smell, touch, and taste) in protecting the healthcare environment.

The contacting of suspicious persons and the investigation of suspicious situations are some of the most important areas of the patrol function. Officer safety is an important discussion early in the career of the new security officer so that the officer can effectively carry out these functions or respond to a critical incident.

### *OSHA Compliance*

Hazard communications, blood-borne pathogen exposure prevention, tuberculosis, universal precautions, and other OSHA-required training is mandatory for US HCFs prior to the security officer working. The healthcare protection administrator must familiarize himself/herself with each of these safety and health requirements and specifically address how initial and annual training will occur.

## IAHSS Progressive Certification Program

The Progressive Certification program of IAHSS is a three-tier training and certification program that helps security officers prepare for and address the special protection needs of healthcare institutions. Providing a foundational understanding of healthcare security, the Basic Training level is the first phase in the IAHSS Progressive Certification program. The Advanced and Supervisory Training levels expand on the Basic Training program and allow security officers to continue their education after becoming certified at the Basic Training level. The programs are designed for the healthcare security officer who desires to achieve higher levels of responsibility in the organization. The following certifications, administered by the IAHSS Commission on Certification, are available:

- Basic Training certification for the healthcare security officer.
- Advanced Training certification for the healthcare security officer.
- Supervisory Training certification for the healthcare security professional.

Each certification is valid for 3 years. Before the certification expires, the individual has the choice of being recertified at the same level or progressing to the next level. Information appropriate to certification for each of these levels is meticulously developed and regularly updated by professionals in healthcare security and safety in the IAHSS training manual developed for that specific level:

- *Basic Training Manual for Healthcare Security Officers.*
- *Advanced Training Manual for Healthcare Security Personnel.*
- *Supervisory Training Manual for Healthcare Security Personnel.*

Many healthcare protection departments are firm believers in promoting from within, and offer compensation increases and advancement opportunities to security officers who complete, and maintain, one, two, or all three levels of IAHSS certification. Healthcare organizations are discouraged from making IAHSS certification a mandatory requirement for their security staff as not all competent security officers are good test-takers.

## IAHSS Basic Security Officer Training

The IAHSS initially developed a 40-hour basic training program for security officers in the mid-1970s. The program, which is actually a standard, has stood the test of time. It has been revised from its previous focus on unit hours to its current certification basis and reflects the changes and evolution of the healthcare security profession. With its fourth edition released in 2007, the *Basic Training Manual for Healthcare Security Officers* continues to represent a consensus of what healthcare security administrators consider a basic training curriculum. The curriculum centers on understanding the healthcare environment and its relationship to security. [Table 9-2](#) presents the sections and subject areas covered in the basic security officer training.

**Table 9-2** IAHSS Curriculum for Basic Security Officer Training

### IAHSS Basic Security Officer Training

- Section One—Introduction to Healthcare Security
  - 1—The Healthcare Organization
  - 2—Security Services in the Healthcare Organization
  - 3—Customer Relations: Public, Employee, and Labor Relations
  - 4—Customer Service
  - 5—Teamwork and the Healthcare Interface
- Section Two—Fundamental Security Skills
  - 6—Patrol Procedures and Techniques
  - 7—Security Interactions in Various Situations
  - 8—Risk Reduction: Restraints, Self-Protection, and Defense
  - 9—Professional Conduct and Self-Development
  - 10—Crisis Intervention
  - 11—Interview and Investigation
  - 12—Report Preparation and Writing
  - 13—Report Value and Liability
  - 14—Judicial Process, Courtroom Procedures, and Testimony
  - 15—Parking and Crowd Control
- Section Three—The Role of Security in Healthcare Organizations
  - 16—Patient Care Units
  - 17—Business Office and Financial Services
  - 18—Pharmacy: Physical Security, Narcotics, and Dangerous Drugs
  - 19—Emergency and Mental Health Units

(Continued)



**Table 9-2** (Continued)**IAHSS Basic Security Officer Training**

- 20—Infant and Maternity Units
- 21—Medical Records and HIPPA
- 22—Support Units and Ancillary Services
- Section Four—Protective Measures
- 23—Vulnerabilities and Risks in Healthcare Settings
- 24—Integration and Use of Physical Security and Access Control Systems
- 25—Equipment Use and Maintenance
- 26—Identity Theft
- Section Five—Healthcare Safety and Emergency Management
- 27—Overview of the Incident Command System
- 28—Basic Safety Protection for the Officer
- 29—Fire Prevention, Control, and Response
- 30—Terrorism
- 31—Bomb Threat Response Planning
- 32—Emergency Management and Response
- 33—Civil Disturbances
- 34—Violence Issues: Domestic, Workplace, and Hostage Situations
- Section Six—Security and the Law
- 35—Criminal and Civil Law
- 36—Statutes and Standards Affecting Security Actions
- 37—Regulatory Agencies
- 38—Public Safety Interaction and Liaison

The successful completion of this training program leads to Basic Training certification by the IAHSS. Certification is granted after the officer passes a closed-book examination consisting of 100 multiple choice questions. The test can be taken on paper or electronically. One need not be employed as a healthcare security officer to become certified; the Association has certified well over 39,000 protection professionals.

Several formats are currently used to prepare the student for the certification examination. One of the most popular is an IAHSS chapter project. This approach ensures a maximum number of students and uses chapter members as instructors and discussion leaders. A high level of training is ensured, costs are shared, and each organization need not devise a unique program. Another format is training through a local university



FIGURE 9-4 Layout and design of the current IAHS Basic Security Officer Certification certificate.

or vocational college. Some colleges offer a regular credit course structured around the standard; others offer an institute-type course that may or may not award credit hours. The college assumes certain standards, which gives the instruction a certain amount of credibility. The student must still successfully pass the IAHS certification examination. In-house and contractor training formats vary from formal classes to facilitated study groups, to supervised self-study, or a combination of these approaches. Figure 9-4 shows the layout and design of the current basic security officer certification certificate.

### IAHS Advanced Security Officer Training

The Advanced Training level is the second phase in the IAHS Progressive Certification program. Now in its third edition, the 2008 *Advanced Training Manual for Healthcare Security Personnel* program curriculum builds on the knowledge and skills developed from the IAHS Basic Training certification. It is encouraged, but not required, that the student complete the basic certification program as a prerequisite to participating in the advanced training program. This program is separated into 14 different subject areas, as shown in Table 9-3.

The successful completion of this training program leads to Advanced Training certification by the IAHS. Certification is granted after the officer passes the 50-question

**Table 9-3** IAHSS Curriculum for Advanced Security Officer Training**IAHSS Advanced Security Officer Training**

- 1—Security Awareness and Crime Prevention
- 2—Enhanced Customer Service
- 3—Premise Liability
- 4—Methods of Patrol
- 5—Investigative Techniques, Reports, and Procedures
- 6—Off-Campus Security and Safety
- 7—Workplace Violence
- 8—Patient Risk Groups
- 9—Interacting with Patients
- 10—Special Security Concerns
- 11—Security in Sensitive Areas
- 12—Electronic Security Technologies
- 13—Critical Incident Response
- 14—Advancing Professionalism

multiple-choice Advanced Healthcare Security exam. The test can be taken on paper or electronically. Once certification is issued, the student is recognized as a Certified Advanced Healthcare Security Officer (CAHSO).

### IAHSS Supervisory Training

The Supervisory Training level is the third phase in the IAHSS Progressive Certification program. Now in its third edition, the 2007 *Supervisory Training Manual for Healthcare Security Personnel* curriculum is intended for persons who are in current supervisory positions or persons who want to prepare themselves for supervision. It has been reported that security staff have also completed this program so that they better understand the supervisory process. It is encouraged, but not required, that the student complete the basic and advanced certification program as a prerequisite to participating in the supervisory training program. This program is separated into 18 different subject areas, as shown in [Table 9-4](#).

The successful completion of this training program leads to Supervisor Training certification by the IAHSS. Certification is granted after the candidate passes the 50-question multiple-choice Supervisor Healthcare Security exam. The test can be taken on paper or electronically. Once certification is issued, the student is recognized as a Certified Healthcare Security Supervisor (CHSS).

**Table 9-4** IAHS Curriculum for Supervisory Training**IAHSS Supervisory Training**

- 1—Introduction to Supervision
- 2—Self-Improvement
- 3—Supervisor Responsibilities
- 4—Civil Liability and the Supervisor
- 5—Employee Relations and Employee Appraisals
- 6—Safety and the Supervisor's Responsibilities
- 7—Planning for Emergency Management and Response
- 8—Developing Training Plans and Programs
- 9—Supervisor Development
- 10—Effective Crime Prevention Programs
- 11—Authority and Control
- 12—Budgeting and Cost Control
- 13—Leadership
- 14—Principles of Customer Service
- 15—Handling Complaints and Grievances
- 16—Professionalism and Ethics
- 17—Communication Skills in Supervision
- 18—Security Operations

Many healthcare protection departments require the completion of all three levels of IAHS Progressive Certification for their security supervisory and management staff.

## Specialized or Supplemental Training

The specialized training developed by the organization is intended to be specific to the needs, philosophy, and concerns of that organization. For example, weapons training would pertain to the use-of-force tools utilized in the security program. Specialized training may also build on areas of basic training provided during preassignment training or in the IAHS Progressive Certification training series. For example, the IAHS basic training includes general crisis intervention; however, a specific organization may want to supplement training in this area by using a nationally recognized program or an in-house developed program.

An example of developing specific programs to be part of the overall security training program can be found at Barnes-Jewish Hospital (St. Louis) and St. Louis Children's

Hospital. There, the security staff researches, designs, and teaches many of what they refer to as “supplemental courses.” At the end of each course, the attendees grade the class and evaluate the instructor from an effectiveness viewpoint. A recent annual training program developed by the security staff consisted of some 11 different training areas, as shown in [Table 9-5](#).<sup>6</sup>

## Contemporary Issues in Healthcare Security Training

The commitment to the ongoing development of security personnel is paramount to the successful healthcare security program. To develop the highest potential in each employee, an organization must offer refresher training throughout the calendar year. This training should update the staff about security protocols and consists of a review of modified post orders and contemporary security topics such as gang activity, infant abduction prevention, emergency preparedness, and terrorism.

### *Gangs*

Gangs, gang activity, and the results of such activities can have a negative impact on healthcare organizations, their employees, and others in the healthcare community. In their article “Gang Culture from the Streets to the Emergency Department,” Bonnie Michelman and George Patak quote the National Alliance of Gang Investigators Association:

*Once found principally in large cities, violent street gangs now affect public safety, community image, and quality of life in urban, suburban, and rural areas. No region of the United States is untouched by gangs. Gangs affect society at all levels, causing heightened fears for safety, violence, and economic costs.<sup>7</sup>*

The issue of gang activity and gang violence is not isolated to just hospital emergency departments. Security staff members in all aspects of healthcare must be trained to identify gang affiliations or behavior and other gang identifiers to include graffiti and hand signs. Further, the training should expand on specific protocol and expectations to be followed on what to do if the security officer encounters a gang member while on patrol or as a patient or visitor to the facility. It is a common occurrence for gang members to impersonate friends or family of a patient or gain knowledge or access to the patient when in fact they may be an opposing gang who is interested in doing harm to

**Table 9-5** Subjects and Topics of an Annual Supplemental Security Officer Training Program

Annual Supplemental Security Training Courses			
Workplace	Security Concerns and Issues		Weapons
Change Management	Domestic Violence	Environmental Issues	Enhanced Firearms
Cultural Diversity	Gang Awareness	Gerontological Issues	Impact Weapons
Service Excellence	Persons with Disabilities	Risk Management	

Source: Adapted from Barnes-Jewish Hospital (St. Louis) and St. Louis Children's Hospital.

the patient or “finishing the job” if the patient is in the hospital due to an attack by the gang.<sup>8</sup> The training provided to the security staff should provide clear guidance on their authority to restrict visitation to a patient, checking all belongings for weapons, placement of the patient under an assumed identification, or introduce extra security precautions if they think a patient or visitor creates an undue risk to the healthcare system.

### *Weapons of Mass Destruction/Pandemic Flu*

In order to effectively manage disasters, healthcare security officers need to learn the ABC of diagnosing exposure models, spotting exposed persons, and donning appropriate contaminant-controlling attire to limit potential exposure. The healthcare security program should establish a Weapons of Mass Destruction (WMD) training program to enhance the organization’s capability of helping contain WMD exposures before they adversely impact the institutional setting.<sup>9</sup> All security officers need to be taught the basic symptoms associated with WMDs and learn to identify the symptoms of exposure—from the most common biological, chemical, and radiological agents, to recognizing the warning signs associated with flu symptoms’ emanating from these contaminant. [Table 9-6](#) identifies a

**Table 9-6** Weapons of Mass Destruction Exposures/Agents Guide

WMD Exposures/Agents			
Biological	Viral	Hazardous Chemical	Radiological
<p>Anthrax—a spore that can create an acute infection of the skin, lungs, or gastrointestinal system.</p>	<p>Ebola—the most dangerous virus known to science; requires direct contact with the blood or secretions of bodily fluids.</p> <p>Smallpox—an infection which occurs from contact with blood, secretions, of bodily fluids or via inhalation from infected persons.</p> <p>Ricin—a toxin made from the leftover mash of the Caster bean, which is processed for the production of the castor oil. Easily accessible and easy to produce. It kills body cells on contact. There is no cure for this toxin.</p>	<p>Cyanide—poisons victims through inhalation of gas. The longer the exposure or the higher the concentration of cyanide, the quicker a victim will be contaminated.</p> <p>Mustard Gas—a blistering agent; it is an oily liquid that is heavier than water. The vapors and/or liquid are the danger.</p> <p>Sarin Gas—a nerve gas; it disrupts the mechanism by which nerves communicate with the organs, causing over-stimulation of the organs.</p>	<p>Radiation Poisoning—is caused by exposure to irradiated uranium that gives off “alpha” and “gamma” rays.</p>

*Concept developed from work created by Anthony J. Luizo, PhD, and Ben Scaglione, CPP.*

basic guideline for WMD exposures/agents that security officers need to learn to identify the symptoms of exposure. All security officers need to become familiar with the decontamination and treatment processes associated with mass casualty or pandemic flu victim incidences.<sup>10</sup>

### *Forensic Patients*

Patient-prisoners pose unique safety and security challenges for healthcare organizations. TJC standard HR.2.10 EP10 requires the organization to “orient and educate forensic staff to include how to interact with patients; procedures for responding to unusual clinical events and incidents; the hospital’s channels of clinical, security, and administrative communication; and distinctions between administrative and clinical seclusion and restraint.” This function is often performed by the healthcare organization’s security staff and tracked meticulously.

Clear direction and guidance help keep everyone safe during the delivery of forensic healthcare. With the safety of patients and personnel as a priority, defining the security officer role in the treatment of inmates and arrestees is especially important, but is all too often missing in the security officer training plan. If security staff are summoned for assistance, what can be provided? Does the organization allow for security staff to provide bathroom breaks or spell law enforcement officials in their duty to watch the patient? CMS differentiates in the use of handcuffs or other restrictive devices applied by law enforcement officials.<sup>11</sup> If security staff are expected to render assistance to law enforcement officials, are there modifications to the use of force continuum that the officer must be trained on?

A challenging issue for security staff is a clear understanding of what patient information can or cannot be disclosed. All too often, law enforcement officials practice a “drop and run” technique. The patient, known to have broken the law, is not arrested or formally charged. The law enforcement officer leaves the HCF with the mandate for the security officer to notify him/her prior to discharge. The issue is the subject for many heated discussions in the healthcare community. Can the security officer legally notify the authorities? The answer is that it depends on the healthcare organization’s policy and their interpretation of HIPPA.

Some healthcare organizations release this information freely to law enforcement, interpreting that the police officer has “a need to know,” while other organizations view the discharge of a patient as confidential medical information that cannot be readily shared. This is a precarious situation for the security officer who needs specialized training on HIPPA rules and regulations and how to maintain collegial relationships and liaison efforts with law enforcement.

More detailed information about the interrelationship of security with forensic patients is discussed in *Chapter 12, Patient Care Involvement*, and *Chapter 13, Public Safety Liaison*.

### *Emergency Preparedness/FEMA Online Incident Command Courses*

In the United States, the Emergency Management Institute of the Federal Emergency Management Agency (FEMA) has developed Incident Command System (ICS) training that

is available and specifically designed for the healthcare industry. The *Introduction to ICS (ISC-100)* is a free online training program that is 2.5 hours long and provides foundational understanding of an ICS for hospitals.<sup>12</sup> Many HCFs require the completion of ICS 100 for all security officers and include the training as part of their mandatory training program.

The follow-up ICS program, *Applying ICS to Healthcare Organizations (IS-200)*, is a 3-hour online program that provides additional training on and resources for supervisory personnel who are likely to have a role in the HCFs emergency operations center.<sup>13</sup> A large number of healthcare organizations require completion of both ICS 100 and 200 for the security supervisor positions and above.

### *Other Important Training Considerations*

The very nature of protecting a healing environment requires the healthcare security training program to cover a wide variety of subjects and procedures. The level of intensity and amount of focused training time dedicated will vary according to the nature of the healthcare organization served and the security risks identified. Other specialized types of training offered by healthcare protection programs might be:

- Active shooter
- Infant abduction and the security officer
- Drug theft and diversion investigation
- Media relations
- Very important patients
- Critical incident response/scene management
- Terrorism awareness in the healthcare environment
- Laws of arrest, search, and seizure

The list of topics can be exhaustive and unfortunately, the level of depth any one healthcare security program may go to is directly dependent on the resources available and allocated for education and training. The resourceful security administrator will take advantage of every opportunity for training and development to occur on a daily basis, whether through formal educational classes or shared insights from fellow security staff.

## Elective Training

Elective training is generally considered to be for individual self-improvement, but may have some relevance to the employee's job. Healthcare organizations may offer classes such as general computer training or CPR/First Aid, neither of which may be required of the security officer's position. There are also numerous 1- and 2-day workshops and seminars offered in communities in which the individual may wish to participate.

## Leadership Development

Investing in the development of its security leaders should be a strategic focus for every healthcare organization. In an industry that is firmly rooted to promotion from within,



this is an excellent way to sustain core values for the healthcare organization and enhance the perception of personal safety and security to all of its constituents.

The people fulfilling the security leadership roles are fundamentally the success of every healthcare protection program. They are the fabric of the security department. Even in the worst of times, they will drive security program success. But who is encouraging their development? This is a question every healthcare organization must address. All healthcare security leaders must build and continually enhance their personal healthcare security knowledge and build their managerial abilities and leadership prowess.

There is no “one size fits all” model for leadership effectiveness. Leadership capabilities are developed over a person’s career, but unlike in sports where there is more time practicing than playing, the role of being a security leader provides very few “practice fields” for leadership to be developed. Healthcare security leaders must strive to raise the bar of professionalism in the security industry, and make a conscious decision to rise above the status quo of our industry. The focus of the leadership training and professional development program should stimulate learning and improve the overall effectiveness of each security leader. The purpose is to improve the overall effectiveness and consistency of each security leader through individual personal development, communication, and specific job training.

## Defining Leadership

Determination of the leadership-developed curriculum and delivery model to provide quality leadership development is challenging. One of the very first steps is to define what leadership means to the healthcare protection program. Leadership is defined as the ability to motivate a group of people to perform above their perceived capabilities to achieve a shared goal or vision. When analyzed closely, it can be surmised that:

- *Leaders must have the ability to motivate others.* Not to be misconstrued as charismatic, healthcare security leaders must be able to get security staff excited about performing their job and its importance to the organization. In short, leaders must have the ability to influence the directions, goals, and efforts of others through means that include, but go beyond, the simple exercise of authority.
- *Leadership is a group activity; it is not about being an individual contributor.* The whole team must perform highly, not just the security leader. Healthcare security leaders must be able transfer strength to everyone in the security department and in the healthcare organization in general. In short, leadership is achieving results through others
- *Leaders must get their team to perform above their perceived capabilities.* When challenged and engaged, healthcare security leaders can elevate security staff members to accomplish goals and objectives they did not think they could achieve.
- *Leaders must have a shared goal or vision.* Security leaders have to take the time to gain a sense of ownership in their team. It begins by establishing a vision of what the protection program could be in the future. Providing a clear, yet simple vision of

what could be achieved if everything went right that people can understand and ties into emotion will drive high performance.

## Leadership Competencies

There are many leadership qualities (competencies) critical to the success of a healthcare security leader. There must be a technical understanding of the discipline of healthcare security and basic business principles that form the foundation for every leader no matter what industry is practiced. Today's healthcare security leader must be emotionally intelligent and should have strong personal and interpersonal leadership skills. Without fail, the most successful healthcare security leaders must have the ability to execute and get things done. Underpinning each of these traits is a values-based foundation that must be followed each step of the way.

Healthcare administrators continue to rank the ability to build relationships (internally and externally), openness to change and growth, courage to make the “right” decision, ability to motivate and inspire others, and the level of self-confidence as the traits and characteristics most highly coveted in their leadership team. Knowledge about the technical aspects of law enforcement or general protection is least desired. Thus healthcare security leaders must continue to develop their business acumen, their personal and interpersonal leadership skills, and their ability to execute to help the healthcare organization achieve the performance and results desired. The security leadership traits and characteristics listed in [Table 9-7](#) are most highly sought after by healthcare administrators.

**Table 9-7** Leadership Success Traits and Characteristics

<b>Business/Technical Knowledge</b>	<b>Personal and Interpersonal Leadership Skills</b>	<b>Ability to Execute</b>	<b>Values and Ethical Foundation</b>
Healthcare Security Management	Emotionally Intelligent	Set Priorities	Sense of Integrity
Security Systems	Good Communicator	Set Expectations	Inspire Trust and Hope
Emergency Management	Self-Awareness	Hold People Accountable	Pump Self-Confidence in Others
Human Resources	Self-Management	Problem Solving	Lead by Example Rather Than Power, Manipulation, or Coercion
Performance Management	Social Awareness	Decision Making	Authentic
Project Management	Relationship Management	People Development	Respect for Others
Information Technology	Ability to Lead Self	Change Management	
Strategic Management	Ability to Lead Others	Succession Planning	
Business Continuity Planning			
Finance/Budgeting			

### *Basic Elements of Healthcare Security Management*

The *Basic Elements of Healthcare Security Management* is a half-day preconference workshop offered by the IAHS at their Annual General Membership Meeting and Seminar each year. The workshop is an excellent introduction to the fundamental elements of managing a healthcare security program. The basic objective of this 4-hour workshop is to bring together individuals who may not be as seasoned as the “old hands” of the field of healthcare security with a focus on the “what” and the “how” as it relates to implementing a healthcare security program. The workshop is specifically designed for the relatively new healthcare security manager and supervisor or facilities manager who has a responsibility in the security arena. This “nuts and bolts” program includes a syllabus and extensive workbook, and shares a wide array of sample security policies, procedures, forms, tools, and training materials, which can be readily adapted to individual healthcare security programs. [Table 9-8](#) provides an outline of the curriculum offered by IAHS.

## Training Resources and Records Requirements

Training does not just happen—it requires considerable planning. The planning begins with identifying the curriculum and the resources available for training. Instructors, lesson plans, training material, methods of presentation, evaluation, competency measurements, and documentation are primary elements of the training program.

### Instructors/Facilitators

As continuing education is prevalent in almost all aspects of the healthcare delivery system, an excellent source of security instructors/facilitators can be found in the organization's staff. Staff are generally quite willing to assist other departments in training, and no one is better able to relate to a specific area's security problems than the person responsible for that area

**Table 9-8** IAHS Curriculum for New Healthcare Security Managers

#### **Basic Elements of Healthcare Security Management Training**

- 1—Development of the Security Program
- 2—Basics of TJC Standards Compliance
- 3—Security Program Documentation
- 4—Security Staff Training/Competency
- 5—Hospital Staff Training/Security Awareness
- 6—Security Officer Selection and Deployment
- 7—Utilization of Physical Security Safeguards
- 8—Current Hot Topics in Healthcare Security

or particular function. Generally, an hour is sufficient to accomplish an acceptable level of general training for a specific operating department or function. One-third of this time might be devoted to explaining how the department interacts as a part of the healthcare team; one-third to the department as it relates to security (vulnerabilities, expectations, policy); and the final one-third to questions by security personnel. This allows security officers to question certain practices and to suggest ways to improve the security posture of the facility. Often, a questionable practice in the eyes of a security officer can be explained by the departmental supervisor, giving security officers better insight into the rationale behind the practice.

The use of in-house staff as instructors has several important benefits. Staff instructors are forced to give some attention to their own work as it relates to security. It may be the first real look they have given to their security vulnerabilities. In addition, rapport often develops between the staff member and the security department and its officers. Finally, staff instructors may come to appreciate the security program more as they relate to the professional approach of a trained security force.

Instructors/facilitators from the community are also available to assist in the training program. Likely sources for instructors include insurance carriers, the Red Cross organization, the OSHA, law enforcement officials, state safety agencies, fire prevention bureaus, community relations agencies, healthcare attorneys, and Offices of Emergency Preparedness, to name a few.

## Training Materials

Most people can listen at 600 words per minute but talk only at 100 to 150 words per minute, and are easily distracted. According to Richard Cook, president of Kottcamp & Young, Inc., a management consulting firm, all knowledge is gained through the five senses. Sight accounts for nearly 85% of learning; hearing, approximately 10%; smell, about 5%; feel and taste, negligible amounts. Thus, in training, one should not rely solely on lectures.

Technology has brought significant innovation to traditional security content development and delivery methods. Computer-based training via hosted e-Learning modules, simulated videos, and self-directed touch screen learning modules have all been combined with traditional instructor-led learning to provide more options to train personnel than ever before. The technology advancement for the training world is only expected to improve while reducing the overall cost of this technology.

Security trainers who want a customized training program can effectively create and use authoring tools that are relatively inexpensive to build and manage. Another option is to use internally produced video presentations. With each of these mediums, one can tailor the information to individual healthcare environments. Healthcare organizations typically have a range of sophisticated video equipment readily available. Interactive video technology, which combines these three tools, is also currently used for a variety of training applications. In addition, many off-the-shelf training videos are available that cover a wide range of healthcare security topics. A subscription training service is available from many e-Learning organizations.

e-Learning and computer-based training is not suited for all types of security training, such as demonstrating competency in physically restraining a patient or demonstrating proficiency with the firearm on the firing range. In addition, there is no opportunity for a trainee to ask questions or benefit from group interaction. There will always be a need for instructor-led training, but much of the basic information a security officer needs can be provided through these mediums. They are less costly and can be excellent resources for remedial or point of need training.



*Training Bulletin*  
August 2009

## Emergency Medical Treatment and Active Labor Act



### EMTALA

Known as EMTALA, the Emergency Medical Treatment and Active Labor Act is a Federal Law that sets standards and guidelines for participating hospitals in regards to emergency medical treatment and stabilizing care. This law establishes an obligation to conduct a medical screening and provide stabilizing care if necessary, regardless of the patients ability to pay for those services. In addition, EMTALA also establishes a 250 yard sphere around the campus in which the hospital is obligated to provide a medical assessment and stabilizing care.

### Security and EMTALA

Security Officers and Managers must be aware of how EMTALA will influence their actions when it comes to removing people from the property, giving trespass warnings, and banning individuals from the campus. Security *must not* refuse entry to the property when someone is seeking emergency medical care. Security also must not remove anyone from the property if they appear to have an obvious medical emergency, even if they are not requesting medical services.

EMTALA requires that hospitals provide a medical screening to determine if an emergency medical situation exists. In general, it is the Emergency Room physician or other designated medical provider that will provide this screening. Security must not get in the business of deciding whether patients are experiencing an 'emergency' condition. If a Security Officer issues a trespass warning, it is important that they notify the individual they may return to the campus for the purpose of seeking medical care. When in doubt, seek the guidance of Hospital Administration when prohibiting individuals from the campus.

### The Emergency Room and Active Labor

Most frequently EMTALA will be triggered when a patient presents to the Emergency Room. Security should remember that it is up to the medical staff to determine if an emergency condition exists. Women who present as being in labor also fall under EMTALA, and must be treated usually until after the birth occurs. Though Security Officers may recognize individuals from previous interactions, they must be allowed to present themselves to medical care providers. If, after receiving an evaluation it is determined that no medical treatment is needed, then Security may follow hospital policies on removing that person from the premises.

### The 250 Yard Rule

You may hear the "250 yard rule" invoked to describe a hospital's obligation to treat patients who present at areas outside of the Emergency Department. This rule establishes a 250 yard sphere from the main building within which EMTALA is triggered. This can include a patient arriving at the main entrance seeking emergency medical care, or a patient who has an emergency medical condition apparent to the average person, even if they are elsewhere on the campus such as the parking lots or other buildings on the campus that are a part of the medical center. This rule generally does NOT apply to other businesses that may be located within the 250 yards, or other medical centers such as doctors offices or clinic that have a separate identity. Your hospital should have a map or policy that outlines those areas covered under EMTALA. Be sure to understand your obligations and responsibilities as outlined by your hospital.

FIGURE 9-5 Example of a healthcare security training bulletin (courtesy of Jonathan Ridpath, CHPA).



*Training Bulletin*  
August 2009

## **Emergency Medical Treatment and Active Labor Act Competency**

1. EMTALA establishes a hospital's obligation to provide emergency medical services.  

True	False
------	-------
2. Security can restrict someone from returning to the property at any time, for any reason.  

True	False
------	-------
3. Only patients who arrive at the Emergency Department fall under EMTALA guidelines.  

True	False
------	-------
4. If you encounter a person on the property who does not appear to be ill or injured, you can ignore their requests to see a doctor and remove them from the property.  

True	False
------	-------
5. A person who is on the ground in the parking lot and is unresponsive falls under EMTALA.  

True	False
------	-------
6. Even if a person is unable to pay, they must be assessed and appropriate treatment given under EMTALA.  

True	False
------	-------
7. A security officer's understanding of this law should override hospital policy.  

True	False
------	-------
8. Security Officers should be familiar with hospital policy as it refers to the "250 yard" rule.  

True	False
------	-------

**FIGURE 9-5** (Continued)

A popular method of training is to include training topics in a periodic training bulletin that supports training and development with up-to-the-minute information to security personnel on a number of related security topics. This method can be used advantageously when security personnel are assigned to different facilities, as in a multifacility security system. [Figure 9-5](#) provides an example of a training bulletin. Training bulletins can be created in-house by security department staff or purchased through a subscription service.

The training program should incorporate the use of role play. The application of a medical restraint, the use of a fire extinguisher, the management of aggressive behavior, all have a classroom component, as well as a need to be actually conducted via a role-play exercise.

## Records

No matter how simple or sophisticated a training program is, proper training records must be maintained. A record outlining the training accomplished by each officer should be mandatory. A sample training record is shown in [Figure 9-6](#).

Training records can be entered into the computer and only printed on demand for a specific purpose. In one program the officer's training record is brought up on the screen during the officer's periodic formal evaluation. In another program, each officer's training record is sent to the officer on an annual basis asking for the officers to review its completeness.

Many healthcare organizations and contract security companies have invested in learning management software (LMS) that ties the performance management process directly to individual security officer training plans. Thus, e-Learning and instructor-led training can be based on each security employee's job role and their current skill set, assigning them exactly the courses and learning activities they need.

A basic industry standard of the IAHS is that the healthcare organization maintains an individual training record. This record is to be provided to the officer upon termination of employment. Legal situations will often focus on the training provided individual officers. Complete and accurate records become very important in these situations.

UNITED MEMORIAL HOSPITAL: SECURITY TRAINING RECORD				
Name:		Employee:		Position:
Date	Subject	Duration	Instructor & Affiliation	Competency Measurement
07/16/09	New Security Officer Orientation Class	4 hours	Smith, T., Security Trainer	Passed Section I Competency = 88% Passed Section II Competency = 95% Passed Section III Competency = 99% Passed Section IV Competency = 86%
07/17/2009	Aggression Management	8 hours	Smith, T., Security Trainer	Passed De-Escalation Competency = 96% Passed Physical Maneuvers Competency = 100%
07/13-15/2009	OJT Checklist	24 hours	Jones, R., Training Officer	Competencies
07/20/2009	Orientation Competencies	n/a	Bailey, E., Shift Supervisor	Passed Orientation Competencies = 94%
08/03/2009	Phase I Competencies	n/a	Sandoval, E., Shift Supervisor	Passed Phase I Competencies = 98%
08/17/09	Phase II Competencies	n/a	Bailey, E., Shift Supervisor	Passed Phase II Competencies = 97%
08/24-25/09	UMH New Employee Orientation	16 hours	Various	Passed Employee Health and Safety Competencies
09/20/09	Phase III Competencies	n/a	Bailey, E., Shift Supervisor	Passed Phase III Competencies = 95%
10/15/09	Taser Certification	8 hours	Smith, T., Security Trainer	Passed Taser Competency = 91%

FIGURE 9-6 Sample healthcare security officer training record.

## References

1. Slotnick, J. A. (2008). The future of security training. *Journal of Healthcare Protection Management, 24*(1), 101.
2. Goodboe, M. E. (1995). Should security practice andragogy? *Security Management, 65*(April), 9.
3. Hertig, C. A. (1989). Education teaches the "whys": Training teaches the "hows." *Security Magazine, 29*(August).
4. Department of Health and Human Services. (2006, December 8). *Hospital conditions of participation: patient rights*. Retrieved June 16, 2008, from <http://www.cms.hhs.gov/CFCsAndCoPs/downloads/finalpatientrightsrule.pdf>. §482.13(f), 115.
5. Department of Health and Human Services. (2006, December 8). *Hospital conditions of participation: patient rights*. Retrieved June 16, 2008, from <http://www.cms.hhs.gov/CFCsAndCoPs/downloads/finalpatientrightsrule.pdf>. §482.13(f), 96.
6. Jackson, F. J., & Locklear, J. M. (1997). A few good men. *Security Management, 41*(9), 89–91.
7. Michelman, B., & Patak, G. (2008). Gang culture from the streets to the emergency department. *Journal of Healthcare Protection Management, 24*(1), 23.
8. Michelman, B., & Patak, G. (2008). Gang culture from the streets to the emergency department. *Journal of Healthcare Protection Management, 24*(1), 29.
9. Luizzo, A. J., & Scaglione, B. J. (2007). Training security officers to recognize the perils of weapons of mass destruction and pandemic flu contaminates. *Journal of Healthcare Protection Management, 23*(2), 1.
10. Luizzo, A. J., & Scaglione, B. J. (2007). Training security officers to recognize the perils of weapons of mass destruction and pandemic flu contaminates. *Journal of Healthcare Protection Management, 23*(2), 2–4.
11. Luizzo, A. J., & Scaglione, B. J. (2007). Training security officers to recognize the perils of weapons of mass destruction and pandemic flu contaminates. *Journal of Healthcare Protection Management, 23*(2), 1.
12. Federal Emergency Management Administration. (2007, May 24). *IS-100.HC introduction to the incident command system for healthcare/hospitals*. Retrieved July 21, 2008, from <http://training.fema.gov/EMIWeb/IS/is100HC.asp>.
13. Federal Emergency Management Administration. *IS-200.HC applying ICS to healthcare organizations*. Retrieved July 21, 2008, from <http://training.fema.gov/EMIWeb/IS/is200HC.asp>.



# Deployment and Patrol Activities

Security operations are primarily concerned with security force deployment, which includes fixed-post assignments, patrols, response to requests for service, providing general services, and response to critical incidents. These areas often overlap, with considerable interaction. Each is dependent on the others for support, and their relationship combines the individual elements into a viable security staff deployment pattern.

How well the security department carries out its assigned responsibility will depend in large part on planning, controlling, evaluating, and modifying personnel in the field. Security operations require changes in operation, however slight, almost daily. The proper deployment of personnel is a key element of an effective protection program and the cost of personnel mandates the efficient utilization as a major responsibility.

Although many healthcare security programs are understaffed, the improper deployment of personnel is a major deficiency in many protection systems. Despite the professional growth of healthcare security—with the availability of written materials, multimedia information, seminars, and consultants—many programs still operate with excessive cost.

The objective method of determining how many security personnel are deployed is first to determine the functions and the activity to be accomplished. Reference to the number of personnel required is a rather inexact measurement; security staffing requirements are better expressed in terms of full-time equivalents (FTEs) or hours of service. Determining the volume of security employees needed to fulfill the master schedule can then be based on a ratio that considers the amount of unproductive time afforded by each security staff member; i.e., required training, absences due to vacation or sickness, etc.

Security staff should ideally be deployed on the basis of objective criterion; however, this is not always the case. A sudden rash of security events, or a major incident, can pressurize administration to respond quickly. The reaction is often the addition of security personnel, either because the security administrator does not know what else to recommend or because the decision is made by someone higher in the organization. It is generally the quickest thing to do. A short reaction time and visible action can be most important under many circumstances.

There is some misconception that adding elements of security following a serious incident will commit the organization to indefinitely continuing the added protection. This is not entirely true unless program deficiencies existed before the incident and the response merely put safeguards in place that should have been part of the security program without regard to the incident.

Public, staff, and patients expect a responsible reaction to a serious incident. The decision to discontinue the added protection, such as adding security staff, must be made based on the current security risks and vulnerabilities. It is recommended that a formal review and evaluation be accomplished after the incident to determine the continuance of the added elements of protection. It is quite possible that this review will result in a program change either on a temporary basis or on an ongoing basis. This review should be documented and should include the rationale for decisions made.

The number of security personnel required is often affected by physical and electronic security applications and organizational policies. For example, the facility that secures its perimeter, designates public entry/exit points, and electronically monitors access usually needs fewer security personnel than does the facility that operates in a generally open environment.

Two factors that should not be left out of the equation in determining the number of officers required are the skill level and degree of productivity of each security officer. A well-trained security officer who looks the part, knows and understands his/her role, and consistently performs at a high level is often thought to be more productive than a “guard” who is not properly trained, supervised, or engaged in his/her protection responsibilities. Many healthcare protection administrators agree that one professional security officer can accomplish more than two security guards. A competitive compensation strategy coupled with a professional security officer training and development program are key strategies for getting a high level of engagement and consistent performance. The issue of security officer staffing levels is also discussed in *Chapter 6, Security Department Organization and Staffing*.

## Flexing the Security Staffing Plan

“Flexing” security staffing due to absences and/or vacancies can create undue risk for a healthcare facility in the event of an adverse security incident. It also creates unnecessary payroll expense for the facility when the *minimum* staff deployment is exceeded. The security staffing plan should not be viewed as a total FTE count allocated to the department, but the complement of staff stated to be on duty at any given time per the master schedule.

Fairly common in the healthcare industry is for the security staffing plan to have two staffing plans—a normal complement of a staff in which the master security plan is based and a minimum staffing plan. For example, the security staffing plan calls for a complement of three security officers around the clock but its staffing minimum is two. Unfortunately, in lawsuits for inadequate security (for example, a visitor assaulted in the parking garage), the risk associated with the minimum staffing model is a plaintiff’s attorney claiming: “if there were three security officers as designed, there is significant propensity that the deployment of that officer could have prevented this crime from occurring.” This argument places credence to the dispute of inadequate security and often results in a higher negotiated settlement if the case is not taken to court.

In short, the protection program should refrain from flexing security staffing for temporary convenience or budgetary constraints. Absences and vacancies must always be filled unless uncontrollable circumstances exist. Minimum staffing levels should not be stated differently from the master security schedule. Security resources are typically prioritized related to business risk and the impact on quality patient care. Expenses associated with security staffing levels must be managed and balanced against the constant pressures of cost containment. The goal is to obtain commitment on the security staffing levels for the healthcare facility and maintain a consistent level of security service.

## Deployment Objectives

The objective of deployment is to provide the right number of security staff at the right time and in the right place. In simplified terms, an officer should not be assigned to check the elevator penthouse when visiting hours are closing or shifts are changing. The four primary goals in deployment are to:

- Assign officers to times and areas of high risk.
- Provide rapid response to critical incidents.
- Cover peak workload times.
- Provide high visibility.

Past incident report records and risk analysis data provide the information required to determine areas and times of high-risk potential. Computer-generated maps have all but replaced the pin map in graphically portraying the types and locations of reported incidents. However, maps, plot plans, and building configuration documents are still useful in portraying certain information. The engineering or planning and construction departments usually have these types of documents already prepared. Incidents should be recorded by time period and type. The accumulated statistical data are useful for deployment planning and for patrolling officers, who can obtain at a glance a picture of the problems in a particular patrol area. This process has been most effective with healthcare facilities that have experienced auto-related thefts and break-ins. Trending the exact location, the make, the model of the vehicle, and the time of day of these troubling incidents have helped many healthcare security programs deploy external security resources to discover the perpetrators, help educate employees on what they can do to help prevent future losses, and identify seasonal trends.

To understand the principle of risk potential, consider a pharmacy that operates between 6:00 A.M. and 10:00 P.M. If there have been no past incidents of armed robbery on which to base a patrol deployment, the risk potential is the guideline. The period from 5:00 P.M. to 10:00 P.M. presents a greater possibility of robbery than during the normal workday. After 5:00 P.M. fewer pharmacy employees are on duty, fewer patrons are in the area, and the hours of darkness naturally provide better escape opportunities.

The expectations of security staff with patient assistance in the emergency department can also have a significant impact on the security staffing plan. It is estimated that 70–80% of hospital security incidents are emergency department generated. Some

hospitals with active emergency departments have reported that their security staff must engage with 5–10% of their emergency care patients or persons accompanying patients. For these hospitals, their volume of security incidents is quite significant and continues to grow at a double-digit growth rate. With the continued reduction of behavioral healthcare funding in the United States, another concerning trend is the growing amount of time security officers spend on average with each at-risk patient in the emergency department. What was historically a 20-minute or less intervention today can consume, on average, more than 7 hours per reported incident. The compounded effect of increased volume and increased time spent can result in a very significant proportion of the total security complement devoted to the management of this patient care procedure. Healthcare facilities frequently differ in opinion on the use of security staff for this patient care issue. However, if security officers are used, their total aggregate amount of time must be accounted for in the security staffing plan.

A short response time relative to critical incidents is an indicator of success for the security program. The entire complex must be patrolled in a manner that provides approximately equal response time for critical incidents from all areas of the facility. As response time is shortened, the probability of successfully handling incidents is greatly enhanced. Minimal response time is perhaps the most important factor that a security force can use to build confidence in the security system. Security and law enforcement groups are often judged more on how long it took them to arrive than on their appearance or handling of the incident.

A common missing component is the routine testing of the time it takes for security officers to respond to critical incidents and routine calls for service. A strategy that works particularly well is to make the random test a TJC performance measurement (or improvement initiative) for the security program. With monthly control tests, the security administrator can quantify this important factor and measure for performance improvement or justify the need for additional security resources.

Covering peak periods of requested and scheduled services is an important goal of deployment. This information is obtained from the facility's previous experience and depends on the functions performed in the protection program. The number of calls for service is an important factor in determining how the organization feels about the security service. A large number of calls for service indicate a high level of acceptance of and confidence in the security department. Response time to provide routine requested services is also important. This response will not be as immediate as that for emergencies; however, a good security force will provide service as soon as possible for even the most routine of services.

Another goal of deployment is high visibility of the security force. This practice provides a maximum protection image and a feeling of security and safety for employees, patients, and visitors alike. The importance of this factor cannot be overemphasized.

## Scheduling the Security Staff

A major administrative function of any security program is that of scheduling security personnel into work shifts. Scheduling of security staff does not mean merely putting

down names to fill in the open spaces on a schedule. Scheduling and post assignment have somewhat the same basic objective of deploying the most appropriate officer to cover a post assignment. Scheduling comes first and generally refers to shifts and days of the week. Post assignment is the utilization of officers who are scheduled for a particular shift. Thus, appropriate staff must be scheduled for a shift before a post assignment can be effected in the proper manner. Scheduling and post assignment are obviously synonymous when there is only one officer scheduled for a particular shift.

In both scheduling and post assignment, administrative factors include skill level, post-specific training, appropriate image, security presence desired (commanding, reassuring, customer service), culture, language spoken, physical ability, and being properly licensed for the assignment if required. All these factors must be taken into consideration, without violating discrimination laws, to assign the best person for the specific assignment.

There are generally two types of schedules—the master schedule, which covers a specific time period in advance, and the working schedule, which is a day-to-day document that reflects the actual officer who filled the specific shift. The master schedule, when properly constructed, can be modified each day to reflect any changes in actual shift and/or post assignment. This record of persons actually filling an assignment, as opposed to the projected persons, becomes the official document of coverage and should be maintained for historical purposes. Compensation records become a backup record to prove validity of the schedule if such verification becomes necessary.

A common mistake found in many security schedules is amending the master security schedule to address the personal needs of an individual security officer. The schedule should always take into consideration a reasonableness factor as it relates to an employee being able to fulfill the shift hours and needs. However, changes made for personal convenience of an individual almost always result in a less than optimum staffing plan; frequently creating vacant positions that are very difficult to fill or unnecessary overtime expense.

For many larger departments, labor management software is used quite successfully to maintain scheduling assignments, post qualifications, and track individual security officer training, certifications, and licensing. The programs can, among other functions, search for open shifts, double assignments for a given officer, and assist in identifying officers available in the event of a vacancy. Off-the-shelf programs designed specifically for the security industry are available. Frequently, these add-on modules are available through the healthcare organization's human resource information system.

There is a contrast in the length of the work shift between in-house and out sourced staffing models. In the common 8-hour shift, the in-house program typically utilizes an 8.5-hour shift, allowing one half-hour for a meal break. The out sourced model generally schedules officers for shift coverage for 8 hours, allowing the officer to take a meal break during paid working hours. The latter approach is the best practice for two primary reasons. The most important reason is that the officer is on duty for the entire shift and is not allowed to leave the property except for work-related purposes. Thus, a meal break can be taken

when the workload permits. The second reason is that the officer is available during the meal break to answer calls for service. In other words, the officer is always in service. This is very important when there is only one security officer on duty at the facility.

The basic reason why most healthcare security personnel are uniformed is to provide visibility to persons being protected and a visible deterrent to the malefactor. Those who are being protected develop a sense of well-being when they can see the security effort in action.

Employees expect to see the security officer at certain times when arriving or leaving the workplace. A problem develops when that officer is called away from normal deployment to perform another activity, such as answering a call for service. Employees might then complain that security personnel are not where they are supposed to be and are thus neglecting their job—or worse yet, a serious incident might occur. There are seldom sufficient security personnel to assure consistent preventive deployment patterns.

An example of employee expectations not being met occurred at a hospital where a female employee was sexually assaulted at the medical center as she arrived at work. In the testimony heard by a jury, the employee stated she had grown accustomed to seeing security every night outside and thus did not overly concern herself with her would-be attacker that she admitted to seeing prior to leaving her car. The external patrol security officer had been asked to stand by to watch an at-risk patient in the emergency care center. Although the jury did not believe the security officer was derelict in his duty to protect the healthcare facility, they determined that if the officer had been performing his normal activities, there is reason to believe that the officer could have prevented the employee from being a victim of crime. As a result, the jury found in favor of the employee and levied a very high award against the medical center.

## Deployment Patterns and Concepts

Although the security vulnerabilities; the use of physical and electronic security safeguards; the layout, size, and location of the facility; and its philosophies are factors that alter security officer coverage plans, some basic deployment patterns can be applied.

In extremely small hospitals that use only 8 hours of security officer coverage per day, the hours from 6:00 P.M. to 2:00 A.M. generally provide the best coverage plan. In this coverage plan, the security officer reports for duty at about the time managers and supervisors are leaving for the day. The officer is present to cover the period of highest patient/visitor load (7:00 P.M. to 9:00 P.M.), and after the majority of visitors are gone, the facility access points can be secured. The officer is then available to assist in evening and night shift changes. The movement of personnel and the requests for services generally settle down shortly after 12:30 or 1:00 A.M., allowing the officer to conduct a thorough facility check before going off duty.

To cover a facility from 6:00 P.M. to 2:00 A.M. 7 days per week, 56 labor hours are required. By extending this coverage by 32 hours per week, the facility can maintain continuous security coverage from 6:00 P.M. Friday to 2:00 A.M. Monday, along with 6:00 P.M.

to 2:00 A.M., Monday through Thursday. Of course, this coverage pattern does not fit all facilities, and the available labor hours must be scheduled for the greatest benefit. If problems develop or new vulnerabilities present themselves, coverage must always be shifted to meet these needs.

One should not think only in terms of 8-hour blocks. A 10-hour shift from 6:00 P.M. to 4:00 A.M. or 5:00 P.M. to 3:00 A.M. would improve coverage significantly over the above-described 6:00 P.M. to 2:00 A.M. plan. The most advantageous deployment plan may require 4-, 6-, 10-, or 12-hour shifts. Split shifts may also be used to great advantage to provide the maximum coverage required. In each, the schedule must consider how reasonable it is that the position can be staffed. Many security administrators have created creative security plans only to find that they cannot keep consistent staff.

Ten-hour shifts have become popular alternatives to the traditional 8-hour shift for several reasons. Employees put a high premium on maximum leisure time. The 10-hour shift allows a 4-day workweek, which in effect yields a 3-day weekend. A 4-day workweek also benefits employees financially by reducing work expenses, such as meals and commuting costs. The 10-hour shift also allows organizations to work an officer 50 hours per week if necessary and still give the officer 2 days off. The challenging aspect of 10-hour shifts is found in the 168 hours of coverage in the 24-hour/7-day-a-week schedule—it is not evenly divided by 10. Thus, a variation in the plan must be created. To offset, many organizations use a mixture of 8- and 10-hour shifts in their master schedule.

## Post Assignments

Security officer deployment plans normally consist of a combination of post assignments. The variety of post assignments can be separated into four distinct categories: fixed post, modified fixed post, sector or zone patrol, and unrestricted patrol. The latter two assignments are often referred to as roving patrols. Each of these post assignments has specific objectives and purposes; however, all are intended to provide a degree of activity accountability. The most accountable assignment is the fixed post.

The fixed post is a stationary post that is located at a specific location for a specific time period. A true fixed post requires the assigned officer to be relieved for any absence whatsoever. The fixed post is expensive and is generally used to provide a certain function, such as an after-hours access control point, staffing of a walk-through magnetometer, operations center, communications control point, or other process center. It is also used to provide a presence or visibility. Officers in fixed-post assignments obviously cannot be available to respond to calls for service. If fixed-post officers respond to calls, employees do not see them, which can lead to complaints and even legal problems should an incident occur while the officer is absent. Employees depend on this protection being in place, but on the other hand they have difficulty understanding why officers cannot leave the post to render routine assistance. For example, an employee who has locked his keys in a car must wait for a patrol officer to be dispatched to render assistance.

A modified fixed post is used in a number of programs. The post is left unoccupied at times to conduct patrol rounds or to answer a call for service. A good example is a modified fixed post located in an emergency department. The security officer may be responsible for the general area, including the parking lots outside the emergency area. The officer may at certain times leave the post to conduct a short security patrol or to assist patients or visitors within the general emergency department area.

Another variation of the modified fixed post is the random rotation to two or more fixed-post locations. For example, three areas of the facility—the main lobby, the patient care tower, and the loading dock—may be designated as rotating posts. Security officers assigned to this type of post divide their time between the three areas on a nonpatterned schedule. They are not free to patrol other areas of the facility; they must be in one of the three designated areas at all times.

Sectored (zone) patrol and unrestricted patrol are basic methods of deployment, but are still considered to be post assignments. The purpose of these roving patrols is to achieve security objectives through security officers who move within prescribed areas. Their actions can be divided into four primary categories: response to critical incidents, inspection services, routine preventive patrol, and response to provide courtesy or routine services. Sectored patrols, in which the patrol area is strictly defined, are used in larger programs when a patrol officer is assigned to a given area for a specific period of time. In unrestricted patrols, officers are free to patrol the entire complex. During any given shift, a single officer may be assigned to a variety of different post assignments.

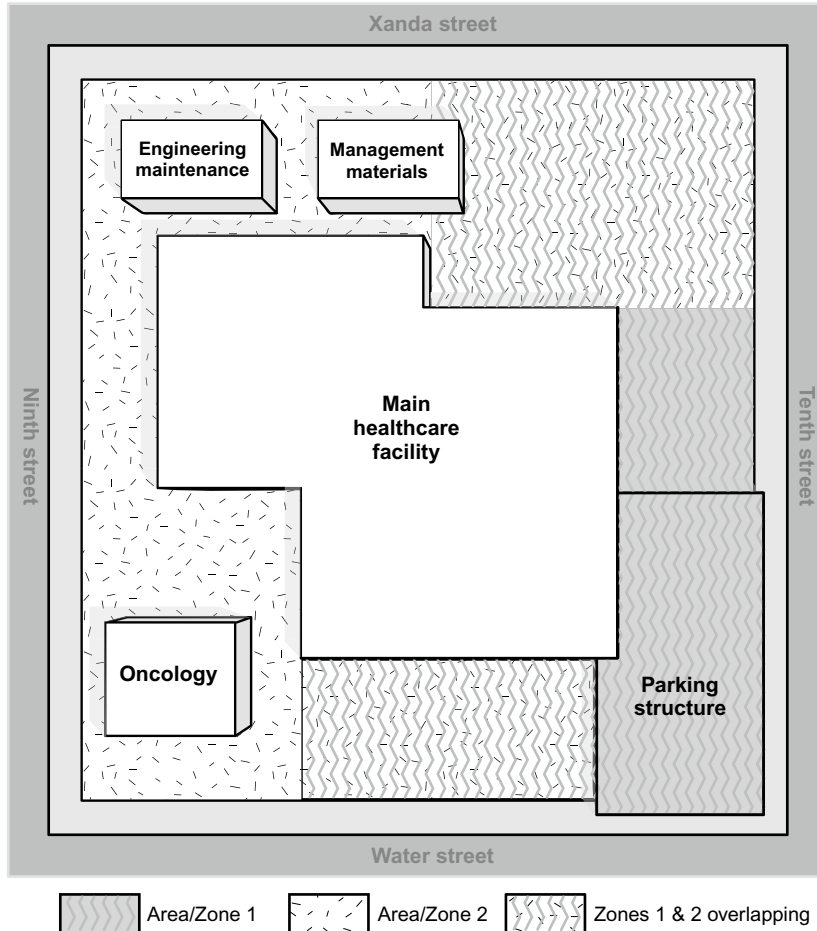
A frequent challenge in today's healthcare environment is how to handle calls for extra staffing. In healthcare organizations providing patient assistance, there is a need for the department to preplan how multiple patient assists are managed. If additional security staff are pulled from the existing complement, arrangements must be made to offset the reduction in force in other areas. How temporary department coverage requests are managed will vary by organization. Some organizations empower their security staff to call in extra security support to include specialized sitters or off-duty officers while other facilities make prearrangements for the external patrol officer to cover both internal and external patrol duties. The important component is that extra security needs occur in every facility from time to time and the security staff should have a clear understanding of the organization's expectation of how it should be managed.

## Basic Patrol Deployment Plans

Security officers who perform patrol duties should be assigned to specifically defined areas. The officers are thus responsible to protect a given area and are held accountable for performing the prescribed activities.

Every facility has certain areas or sections that require a greater frequency of patrol. These more vulnerable areas can often be serviced by overlapping patrol patterns, shown in [Figure 10-1](#).





**FIGURE 10-1** Overlapping security patrol areas.

Patrol area assignments may be altered for various shifts or during shifts in response to the number of personnel assigned to patrol an area or to variations in vulnerability. For example, a facility with two patrol officers on the 4:00 P.M. to 12:00 A.M. shift may deploy one officer internally and one externally, except for various times when parking lots and other external areas are vulnerable to assault, vandalism, or breaking and entering of vehicles. At these times, both officers may be deployed to the external campus. The following schedule illustrates how such a deployment plan might work.

Patrol Officer One	
4:00 P.M. to 5:00 P.M.:	Entire grounds and parking areas
5:00 P.M. to 7:00 P.M.:	North half of external area

7:00 P.M. to 10:30 P.M.:	Entire internal area
10:30 P.M. to 12:00 A.M.:	South half of external area
Patrol Officer Two	
4:00 P.M. to 5:00 P.M.:	Entire internal area
5:00 P.M. to 7:00 P.M.:	South half of external area
7:00 P.M. to 10:30 P.M.:	Entire grounds and parking area
10:30 P.M. to 12:00 A.M.:	North half of external area

In this example, each of the officers patrols both internally and externally. This allows the officers to patrol the same area so that one may find a condition or problem the other officer may have missed. It is also desirable that the officers share in the exposure to adverse weather conditions.

Another method of providing increased patrol coverage is to assign to one officer a patrol area that covers two or more smaller patrol areas. This type of deployment is commonly assigned to a patrol supervisor; however, this is not always the case. The patrol officer assigned to the large patrol area not only provides extra patrol, but also acts as a backup officer for each of the smaller patrol areas. Backup assistance is provided without diverting another patrol officer from his or her assigned area and possibly leaving that area void of security coverage.

## Double Coverage

A general principle in deployment is to maintain a 24-hour coverage schedule, 7 days a week, before deploying more than one officer on a given shift. However, double coverage may be used to good advantage when building a 24-hour program while the number of hours authorized is slowly increased. For example, a program authorizing 112 hours of coverage may find that a coverage pattern of 4:00 P.M. to 12:00 A.M. and 10:00 P.M. to 6:00 A.M. is more productive than 4:00 P.M. to 12:00 A.M. and 12:00 A.M. to 8:00 A.M. The double coverage during the late-night shift change may be more important than the 2 hours from 6:00 A.M. to 8:00 A.M.

In many medical centers, security officers' shifts begin at 8:00 A.M., 4:00 P.M., and 12:00 A.M. These times work quite well in general hospitals or nursing homes because they follow the major shift changes of facility staff by approximately 1 hour. A change of security personnel is thus avoided when most facility staff are in the process of changing shifts. Today, there are fewer concentrated shift change times because medical center programs use many different shifts.

Table 10-1 shows a deployment plan for a medium-sized medical care facility utilizing all 10-hour shifts.

Table 10-2 shows a deployment plan for a small medical care facility. In the staffing plan, there is double coverage for the 10:00 P.M. to 12:00 A.M. shift change. In this plan, which uses 182 hours of coverage per week, 8- and 10-hour shifts are involved.

**Table 10-1** Sample Staffing Plan for a Medium-Sized Medical Center

Shift	Day of Week/Officer Assignment						
	Sun	Mon	Tues	Wed	Thurs	Fri	Sat
6 A.M.–4 P.M.	1	1	1	1	2	2	2
6 A.M.–4 P.M.	2	3	3	4	4	4	4
2 P.M.–12 A.M.	5	5	5	5	6	6	6
2 P.M.–12 A.M.	6	7	7	7	7	8	8
10 P.M.–8 A.M.	9	9	9	9	10	10	10
10 P.M.–8 A.M.	10	11	11	12	12	12	12
7 P.M.–5 A.M.	13	13	14	14	14	13	13

**Table 10-2** Sample Staffing Plan for a Small Medical Center

Shift	Day of Week/Officer Assignment						
	Sun	Mon	Tues	Wed	Thurs	Fri	Sat
8 A.M.–4 P.M.	2	1	1	1	1	1	2
4 P.M.–12 A.M.	3	3	5	5	3	3	3
10 P.M.–8 A.M.	4	6	6	6	4	4	4

## Operational Versus Nonoperational Times

Medical centers operate on a 24-hour basis. However, each healthcare facility can define an operational time period and a nonoperational time period. As with so many other concepts, these time periods vary to some degree from organization to organization, with some quasioperational periods falling between the operational and nonoperational periods. These time periods have a direct implication for patrol deployment. During the operational time period, the patrol officer is a support element to be called on for assistance and to provide a general surveillance of public and general-use areas. The operating concept is that departments require little if any internal patrol when they are fully operational.

During the nonoperational time period, the patrol officer and the entire security function take on a custodial role in protecting the facility. Many departments are closed, and officers must check these areas to ensure that they are secured properly and to question strangers in the area. In other words, the security staff must understand what is normal for the department so that they can more readily recognize what is out of the ordinary.

One must first review the complex as a whole and then each area or department to determine the security officer's proper role for a given time period. For general hospitals, the operational period is usually from 6:00 A.M. to 5:00 P.M. The transition period between

5:00 P.M. and 9:00 P.M. may present some unique security vulnerabilities because some departments are less controlled than they are during the true operational time period. During this transition period, there is enough people traffic within the facility to provide would-be malefactors with anonymity and a possible “ruse purpose” for being in an area. After 9:00 P.M. facilities generally close their doors for the night. Of course, some departments do operate with reduced personnel on duty or on call. For example, Central Supply may operate 24 hours but reduce staff to only one or two persons during the late-night hours.

Security officers must constantly monitor the status of their assigned area and alter their patrol activity in relation to this status. If a particular department is open after the normal time period, the officer checks the area more frequently to make certain that the department is secured as soon as possible after it closes. Also, more frequent checks may be required due to the limited personnel on duty as in the case of the Central Supply example.

Weekends and holidays also present special problems. These periods can be categorized as quasi- or semioperational periods for most facilities. Many departments are closed, yet visitors are numerous, and the routine of patient care continues. An added factor is that supervision and facility staffing are reduced to a minimum during these times. These considerations strongly suggest that increased patrol coverage is necessary on weekends to provide the required protection level. The assignment of too many part-time or inexperienced officers during weekends and holidays should be avoided. Note that in the sample staffing plans provided in Tables 10-1 and 10-2 special effort has been made to identify part-time employment opportunities during traditionally low security incident activity periods combined with a reasonableness factor to part-time employee availability.

## Patient Care Units/Areas

Generally, no part of the facility should be off-limits to security inspection. On the other hand, a patrolling security officer has no business entering the pharmacy or narcotic vault, surgical suites, examination rooms, labor rooms, or other similar areas while they are in use. Security officers called to one of these areas should be knowledgeable about the procedures required for entering the area and the proper attire to be worn.

The need to patrol the corridors of patient units varies somewhat with the time of day. During the operational period, when units are fully staffed, there is generally little need for a security patrol. If security services are required, unit personnel should request the needed security support. During the nonoperational period, the increased security patrol of patient units provides support to the limited staff, and the visibility of the patrolling officer creates a greater feeling of safety for the staff. The deployment pattern for the patrol of nursing-care units should be planned in coordination with the nursing service administrative staff. Care should be given so that volume from radio traffic is not disruptive or irritating to patients, visitors, or staff while on patrol.

Historically, stand-alone behavioral healthcare facilities and in-house behavioral health units preferred to not have patrolling security officers on their unit for fear that the

uniform may have an antagonizing or disruptive presence to the patient. Recently, indicators reversing this traditional thought process have been noted. Leaders of the behavior health unit are starting to request more security patrol and increased security officer presence with the patients on these units. More aptly found on transitional care units, the command presence of the security officer in traditional uniform is believed to be therapeutic and helps the patient assimilate to the “real world.”

## Entrances and Exits

If all the people entering and leaving a medical care complex could be properly surveyed and controlled, the protection level would be quite high. It is virtually impossible to achieve this state of control, although some facilities with strong visitor control systems do control a high percentage of the people entering the facility and a somewhat lower percentage of those exiting. Very few healthcare organizations impose this rigid control and instead the healthcare environment too often provides numerous entrances and exits for the convenience of everyone—unfortunately this includes intruders. While relatively free access to hospitals may be the norm during the day, there is a need to reduce this uncontrolled access during the evening and night hours. A general plan is to lock designated entry points at 6:00 P.M. and to further lock down access points at the termination of designated visiting hours. All facilities should designate specific controlled night entrances for late-night visitors, delivery, and others.

Greater patrol time should be allocated to the main entrances and exits and to external patrol than to internal areas when the entrances and exits are uncontrolled. Because officers cannot be in all places and see all things at all times, their patrols should be structured to view as much activity as possible. An officer who checks a busy entrance or surveys two or three exits from the exterior will be able to observe many more people than when patrolling in a far removed area of the facility. The distant areas are, of course, important in the total patrol deployment plan, but they should not receive attention out of proportion to the objective of surveying and controlling the general-use areas.

## Basic Patrol Concepts

The backbone of the security effort is the security officer on patrol. A major objective of healthcare security is to manage the patrol responsibility so that officers maximize time spent on patrol and reduce time spent writing unnecessary reports or doing other non-productive busy work. Patrol can best be examined by the separation of patrol into external and internal considerations.

### External Patrol

External patrol generally covers the grounds, parking areas, and streets surrounding the facility buildings. External patrol is intended to protect vehicles and people entering or

leaving the grounds, to provide surveillance of people attempting to use unauthorized exits, to prevent the unauthorized removal of property from the facility, to prevent or discourage unwanted people from entering the facility, and to provide various courtesy services.

Officers on external patrol provide perimeter security protection. They can often observe much more activity than officers on internal patrol. Not only do the grounds typically offer a much greater area to be vandalized, but officers also have a view of a large area. For example, from a parking lot, an external officer may be able to see three or four hospital entrances and exits, while an internal officer can generally only observe one of these points at a time.

A major responsibility of external patrol is to ensure the integrity of facility access points by frequently checking doors, windows, roof access, and fire escapes to preclude unauthorized use. A common problem is emergency fire exits that are not intended to be used for entry. Although locked from the exterior, these doors often do not latch properly after an exit. In addition, employees and others sometimes place an object between the door and the frame to keep the latch from engaging. This is often done for convenience and not with the intent to compromise security. Nevertheless, this careless act can provide the access needed for an outsider to commit a serious crime. In addition, all fire emergency exits should be alarmed and monitored.

## External Patrol Vehicles

The basic types of external patrols are foot patrols, bicycle patrols, vehicle patrols, personal transport vehicles, or a combination of each. Regardless of the type of vehicle used for patrol, they should be easily identifiable as security vehicles. To be an effective deterrent, it is not enough that the protection capability is present. It must also be highly visible to the people being protected and to those who might be contemplating a criminal act.

Various types of patrol vehicles have their own advantages. Facilities composed of many streets and roads, large and decentralized parking areas, and multiple buildings generally use an automobile or a four-wheel drive vehicle for security. Smaller facilities may find a small golf-cart-type vehicle better suited to their purposes. The use of mountain bikes to patrol continues to grow in popularity in the healthcare environment and is an excellent alternative for campus environments that have many high-traffic sidewalks, surface parking lots, and public thoroughfares in a contained space. A recent trend is the deployment of personal transport vehicle into the security operations of healthcare campuses. A complement to traditional foot patrol, Bryan Warren, CHPA, Corporate Director of Security at Carolinas Health System in Charlotte, NC, has stated that when his officers started using personal transporters they “were able to complete their patrol routes in approximately half the time than they did on foot.” [Table 10-3](#) provides a brief overview of the advantages and disadvantages of various external patrol vehicles.

### *Vehicle Patrols*

Many modern medical facilities occupy large expanses of property and require motor vehicle patrol to ensure proper coverage. Vehicles increase officer mobility, can provide

**Table 10-3** Advantages and Disadvantages of External Patrol Vehicles

	Patrol Vehicle			
	Automobile	Golf Cart	Bike	Segway
Visibility	Good	Fair	Very Good	Very Good
Ease of Use	Good	Good	Fair	Fair
Professional Image	Good	Fair	Good	Good
Areas Traveled	Fair	Good	Very Good	Very Good
Personal Safety	Very Good	Fair	Fair	Fair
Comfort	Very Good	Good	Fair	Fair
Inclement Weather	Very Good	Fair	Poor	Fair/Poor
Transport Others	Very Good	Good	Poor	Poor
Vehicle Assistance	Very Good	Good	Poor	Poor
Environmental Impact	Poor	Fair	Very Good	Good
Total Cost of Ownership	Fair	Poor	Very Good	Fair

protection from the elements, and allow officers to carry the necessary equipment to provide an efficient and effective response to emergencies.

Contrary to the typical police sedan found in many law enforcement agencies, the best security patrol vehicles have a short wheel base to help the driver better maneuver in tight spaces. The “cross-over” lines of vehicles are favored as they provide the driver with additional clearance than traditional sedans. The added height when combined with an amber-colored light bar makes the vehicle more readily visible when on campus. Many healthcare organizations using the security patrol car have experienced significant improvement in security visibility when the light bar is turned on for all external campus patrols.

Although sharing a vehicle between the security department and another hospital department is usually a poor idea, it is possible to provide temporary markings for each type of use. Magnetic signs, available in assorted sizes, colors, and formats, are commonly used. When the vehicle is assigned to the security department, the security signs are applied, and when the vehicle is turned over to another department, the security signs are removed.

The security patrol car should be regularly maintained and kept clean. The image associated with a security patrol car sends a powerful message about how serious security is taken at the facility. A dirty vehicle, faded security markings, missing hubcaps, or the continued use of spare tires each gives negative symbolic gestures that must be managed daily. Individually and collectively the perception of the security patrol car can signal organizational security readiness or a lack of focus on protection services.

### *Security Carts*

Small electric and gasoline-powered vehicles are popular, especially in warm climates. These vehicles have several advantages: they are economical to operate, maneuver well in tight areas, and can generally be driven on grass or landscaped areas without causing damage. With various engine power options, these vehicles can be purchased “street-legal.” When appropriately registered, the street-legal security cart can be driven on public roads.

The security cart can be used in reasonably inclement weather with options available for all-weather enclosures and heating and air-conditioning. These options become important considerations if the cart is routinely used to provide security escorts. Frequently used in healthcare organization for shuttle/transport service and general support services, carts are available in many shapes and sizes. Most security carts cannot carry the service equipment typically found in the security patrol car.

The security cart is often the least visible of all of the external security patrol vehicles listed. Care must be given to readily identify the vehicle with appropriate security markings. Many healthcare organizations equip the golf cart with an amber-colored light bar similar to the traditional security patrol car to maximize visibility.

The ongoing maintenance of the security cart continues to plague many healthcare security operations where they are used. A security cart used daily for external patrols will typically need to be replaced on average every 2–3 years. Thus, the total cost of ownership of the security cart is the least economical of all external security patrol vehicles.

### *Bicycle Patrol*

Bike patrol is an urban and campus patrol concept that focuses on being a visible deterrent to campus crime and an approachable source of assistance and information on the healthcare campus. Bike patrol officers can see over the heads of most pedestrians and over most vehicles. The bikes also provide speed and mobility through crowded and narrow corridors. Bike patrol officers can patrol large areas more frequently in shorter periods of time than gas-powered alternatives, thus being more visible and accessible to the general public.

Patrols on bikes are friendlier; security officers become more approachable and less threatening. A common statement heard from healthcare organizations who have introduced bike patrol is that it allows their officers to be more interactive with the community served while increasing their knowledge of the campus and constituents through positive contact. Kent Hospital (Warwick, RI) President and CEO Mark E. Crevier noted that the bike patrol introduced at his hospital in October 2006 is an example of the hospital’s commitment to “progressive (and) responsive services.” Crevier stated that the bike patrol “help(s) support traffic flow, render assistance and further extend the presence and effectiveness of our security force.”<sup>1</sup> Additional benefits of the bike patrol program commonly include:

- Greater opportunity to be exposed to the public, more accessible image;
- Greater maneuverability in small areas compared to a security patrol car;



- Added element of surprise to counter criminal activity;
- High visibility and crime deterrent.

A healthy and “green” alternative to external patrol vehicle options, most healthcare security departments deploying bike patrol officers frequently get ample volunteers for the special duty. The cycling helps the officer get fit and stay in shape while getting paid. Bike patrol is not for every security officer and should not be mandated. Every bike patrol officer should submit to a human performance evaluation, designed specifically for the bike patrol program, prior to riding on behalf of the healthcare organization.

A bicycle patrol program has specialized training needs. Most certified bike patrol training programs entail between 16 and 32 contact hours and typically emphasize community enforcement concepts, urban safety, and defensive tactics. For personal safety reasons, security officers performing this function should be issued a specific security uniform that can stand up to the mobility requirements of the bike patrol function and withstand the additional wear and tear often found by its riders. All officers should be required to wear a helmet and sign a safety affidavit prior to working in a bike patrol capacity.

In areas of inclement winter weather, many healthcare security programs only use bike patrols seasonally or as weather permits. In the event the bike cannot (or should not) be ridden, the external patrol officer typically transitions into a security patrol car or to foot patrol.

### *Personal Transporter*

The personal transporter (PT) use in healthcare is limited to some of the most innovative security programs, such as Johns Hopkins, Loma Linda Medical Center, Carolinas HealthCare System, and Baltimore’s Sinai Hospital, but is quickly growing and expanding its use in the healthcare environment. The mode of patrol offered by the PT is the most versatile of each of the security patrol vehicles. Unlike motorized vehicles and bicycles, the PT can be used for both internal and external patrol and allow for security officers to patrol open pedestrian environments that are closed to vehicle traffic and respond quickly to emergencies. An alternative to gas-powered vehicles, the electric-powered PT does not emit any carbon emissions, is very quiet compared to other forms of transport, and uses a rechargeable high-capacity battery that can be replenished via a standard 110v outlet, thus further reducing any harmful effects on the environment.<sup>2</sup>

The visibility of the PT is very good as the patrolling officer stands on the vehicle; increasing his or her height approximately 6 inches. Typically well marked as security, the PT is obvious to patients, staff, and visitors alike. This not only adds to its preventative presence, but also makes the officers more approachable as curious patients and visitors tend to ask about these devices when they encounter them.

Using transporters, security staff are also more alert and less fatigued when they have to respond quickly to a situation versus running or pedaling on a traditional bicycle.<sup>3</sup> The PT operator does require specialized training, but by working with the manufacturer,

“train the trainer” sessions can be set up to allow for the creation of in-house trainers which can greatly reduce any logistical challenges for programs with higher turnover. Such training sessions typically involve familiarity with the nomenclature and balancing/use of the transporter, low- and high-speed steering and maneuvering, auto safety shut-down procedures, and general operator safety and troubleshooting. Such training should be performed initially prior to a security officer being allowed to use the transporter, with an annual refresher.

## External Patrol Services/Considerations

Often, the external patrol officer will perform additional services to improve public perception of safety on campus. These include battery-jumping service and transportation of people. There is also equipment that the security staff should have readily available and an understanding of how to operate patrol vehicle(s) used by the healthcare protection program.

## Battery-Jumping Service

Every security department that uses vehicles for patrol service must decide whether battery-jumping service will be provided. Battery jumping is unquestionably a burdensome task. On the other hand, helping a stranded motorist with a dead battery can enhance public relations.

A main factor to be considered is whether the service can be completed safely and without an appreciable decline in the primary protection effort. A nurse stranded in a parking lot at 12:30 A.M. presents vulnerability. The patrolling officer who provides a jump-start performs a good employee relations activity, while eliminating the vulnerability.

Jumper service continues to decline due to more and more costly claims of damage to the electronic computers now found in most vehicles. Improper charging procedures can result in substantial damage. If, however, an organization does decide to offer jumper service, the next step is to establish ground rules, including:

- *Charge:* Will there be a nominal charge for this service or will it be provided at no charge? Most programs do not charge for this service.
- *Hours:* During what hours will the service be provided? This may depend on the hours the patrol service is in operation; however, definite hours of service should be established. A general rule is to provide this service when commercial services (garages and service stations) are closed. In some facilities, the maintenance department provides this service during the day and the security department picks up the responsibility at night and on weekends.
- *Waiver of responsibility:* Motorists who need help should be asked to sign a statement waiving responsibility for any claim that may result from the service to be provided. The legality of the statement in court may be questioned; however, it does provide tangible evidence of intent.

- *Transportation of stranded motorists:* At times, a jump-start service is not sufficient to get a vehicle going. The security department should have a firm policy on providing transportation for stranded motorists.
- *Amount of service:* This service should not develop into a mechanic service, and a policy is needed to ensure that this does not happen. Any service can develop expectations in the mind of the recipient of the service that go beyond the intent of an emergency service.
- *Proper equipment:* The security department should not cut corners on the equipment used for the jumping batteries. Several commercial-type equipment hookups are available that are easy to operate with few mistakes.

### *Transporting People in Security Vehicles*

Guidelines must be established covering the use of security vehicles to transport people other than security personnel. Without a clear-cut policy, the security patrol may find that it has developed into a taxi service, and it is often difficult to cut back on this service once it has been established. In some circumstances, however, transportation service is in the best interests of all concerned.

The transportation of people, other than through planned shuttle operations, should be properly documented. The names of those transported, the reason, the times and dates, and the mileage should all be recorded except where security is providing a routine shuttle-type program.

An example of how the transportation of people can positively affect hospital operations and protection is found in a large medical center in Wheatridge, CO. The hospital had a patient wait time concern that was in part based on the issues surrounding the delay in the pick-up of medically cleared patients awaiting transport to a local alcohol detoxification center. The security department, recognizing and understanding the dilemma, introduced a plan to transport these patients to the detox center. For less than 2 hours of off-campus transportation time every day, the protection program was able to justify the additional expense of a custom-outfitted security patrol vehicle and officer/driver that significantly increased its external security presence on campus. The return on investment was less than 18 months as the hospital could more rapidly turn over the patient care beds in the emergency department.

### *Equipment for Security Patrol Vehicles*

The type of vehicle used for patrol should be selected for the function to be accomplished. In the same manner, the security equipment carried within the vehicle, when possible, should also be tailored to the function. Security patrol vehicles should have the following essential items:

- Communications device;
- Spotlight (fixed or plug-in type);
- Fire extinguisher(s);

- Blanket;
- Chain or heavy tow cable;
- Rope and traffic cones;
- Basic tool set (screwdriver, pliers, etc.);
- Small broom and dustpan;
- Extra flashlights or hand lanterns.

Optional items include a first-aid kit, flares, jumper cables, resuscitation equipment, and air packs. When possible, equipment should be affixed to the vehicle to keep it from rolling around. One security department mounts its equipment on a flat board with tie down straps and boxes constructed to hold specific pieces of equipment. The board can be easily removed and used in another vehicle, if necessary. Equipment boxes are also quite useful.

### *Operating the Vehicle*

Security personnel operating a security vehicle must generally observe all the rules and regulations that apply to private motorists. Rarely do ordinances or statutes classify security vehicles as emergency vehicles. Security officers may feel that their function gives them special driving privileges. Individual officers should be held responsible for any moving violation or parking ticket received while operating a facility-owned security vehicle. A state motor vehicle check of each officer who operates a vehicle should be accomplished on an annual basis. Many insurance companies require this type of periodic check and initial as well as annual driver safety training.

### *Damage to the Vehicle*



Security personnel should be held responsible for any damage to a vehicle in their care, custody, and control. Officers should completely inspect the vehicle before use. This inspection is often documented on the officer's patrol or daily activity log or a specific vehicle inspection form may be used. [Figure 10-2](#) is a sample of specific vehicle inspection report. All vehicle damage reports should be reviewed by an accident or property damage review board to determine whether the accident or damage was preventable and, if so, to recommend action. The action may be a change in procedure or a recommendation for further training for the individual responsible. In some review programs, the responsible party is required to pay for some or all of the loss.



## Canine Patrol

There continues to be a limited but growing use of canine units in healthcare protection programs. They have proven quite effective as a supplement to officers on foot or vehicle patrol. In addition to being a good public relations tool, canines are effective in soliciting cooperation with stressed visitors as well as de-escalating uncooperative persons and other malfeasance in the healthcare environment. Richard Ortiz, Security Director of Banner Health's Thunderbird and Estrella Hospitals in Phoenix, says, "the presence of canines in the emergency department waiting areas can change the attitude of hostile

Vehicle Spot Check

	<b>Date:</b>		<b>Time:</b>	
Vehicle Number:				
Driver:				
Location:				
Odometer:				
Coupon Mileage:				
Inspector:				
Inspection Score:		0		

Answer Yes or No			
	Yes	No	Comments
Up to Date Maintenance			
Current Insurance Card			
Correct Fuel Card			
Maintenance Packet			
Current Registration Card			
Current Stickers on Plate			
Floor Mats			
Damage Outside			
Damage Inside			
Lights Working			
Hub Caps Missing			

Ratings 1–5 (5 is Good)		
		Comments
Clean Inside		
Clean Outside		
Wear & Tear Inside		
Seat Cover Condition		
Outside Condition		
Inside Condition		
Decal Condition		
Tire Condition		
Smoking Evidence		
<b>Total</b>	0	

**Notes**

FIGURE 10-2 Sample vehicle inspection report.

individuals.”<sup>4</sup> As a result, canine programs have proven to be very effective in health-care communities with an active gang presence. In the gang community, it is culturally acceptable to be afraid of a dog but not necessarily a security officer. Gang members would rather deal with an armed security officer than take a bite from a dog.

Dogs offer several patrol advantages. They protect officers on patrol and generally make them more productive while they conduct their rounds. Dogs can often detect the presence of a person hiding when security staff cannot observe the person. Once trespassers or criminals have been observed, dogs have often been responsible for preventing an escape that otherwise would have occurred.

Obedience is vitally important in a canine patrol program. The dogs interact with the public on a day-to-day basis and should receive continual training on when it is OK to bite in addition to other specific commands. A basic argument against the use of dogs in security is the risk of the dog injuring someone. A few documented cases indicate that this can be a problem, although these are few in number. However, it is difficult to apply any meaningful security measures without assuming some degree of liability. One should always be conscious of the liability of protection system elements and should minimize the liability exposure as much as possible.

A canine program can be very expensive to operate, especially in terms of cost benefit. In most canine programs, the dog is utilized exclusively by one handler, which has a variety of associated costs. Rarely do several handlers utilize a single dog. An organization can purchase its own dogs or can lease dogs on an outsourced basis. The outsourced basis is a good method, as costs can be more readily projected and there is much less administrative support required. An organization that owns its own dogs and provides proper training (training is almost always outsourced) can project an annual cost of \$12,000 to \$15,000 for each dog. This does not include the training cost of the handler or the department administrative time. During the course of a typical 40-hour workweek, the handler and dog often work only 32–36 hours per week with the remainder designated for training without incurring additional overtime expense. As a result, some healthcare organizations use 12-hour shifts for the dog and their security officer handler.

When all the advantages and disadvantages of using a dog on patrol have been fully analyzed, there is no (almost) question that their presence produces a sharp reduction in security incidents. In terms of cost benefit, the use of dogs in the healthcare environment can only be justified in a very few programs. To offset the expense, some organizations have applied a shared service approach to canine patrol. Most effective for multicampus health systems or medical campuses with multiple facilities, the incurred costs of the canine program is shared among a group of healthcare organizations. The basic premise of the shared service approach to canine patrol is available for all locations as situations arise or on a random patrol basis.

## Internal Patrol

Effective preventive patrol is the backbone of a deterrent program. Patrol is not just walking down a corridor or through an area; it requires being alert and checking and observing

with all five senses. The security officer should always have a purpose for inspecting each department or area of the medical complex. This purpose will vary from area to area, but generally the security officer will:

- Check to see that the people assigned to an area are not in need of help (i.e., sick, injured, or being victimized);
- Practice conservation (check water or fuel leaks, unnecessary lights or windows left open, unfamiliar equipment noises);
- Look for safety hazards (moisture on the floor, holes, protruding hazards, or malfunctioning lights);
- Inspect for fire safety (undue accumulations of combustibles, blocked exits, extinguishers that are out of place or show evidence of use, doors opening in the wrong direction, sticking or malfunctioning locks, and smoking violations);
- Watch for evidence of unauthorized people or unusual physical factors;
- Watch for signs of theft or unauthorized removal of property;
- Be alert for acts of malicious destruction, horseplay, consumption of intoxicants or drugs, boisterous conduct, and secure items or equipment that may have been inadvertently left unattended;
- Ensure that all doors are secure at the appropriate time and follow through with periodic inspections;
- Check out-of-the-way places and know where each door leads and how to reach every part of the medical care complex;
- Answer questions for visitors, employees, and patients; direct and escort them;
- Be available for service; if an officer is in doubt as to appropriate action, he or she should check with a security supervisor or perform the duty and check afterward for future clarification;
- Frequently check locker rooms and public washrooms;
- Enforce hospital rules. To enforce rules properly, it is essential that security officers always abide by the rules and by security department regulations (authority is easily abused, and nothing creates resentment as quickly as the misapplication of authority).

It is impossible to list all the areas or conditions that should be inspected. Every facility has unique characteristics that require special patrol activity. The one common area that should be patrolled in all facilities are the stairwells, storage areas, and other out-of-the-way areas. A woman being treated for a stomach ailment disappeared from her 7th-floor room in a Nashville, TN, hospital. Sixteen days later, a nurse noted a foul odor; the missing patient's decomposing body was found on the 10th floor in a storage area. In another case, a man was missing for 5 days after failing to show up for a hospital medical appointment. He was later found dead in a stairwell by a housekeeping employee.

The trash collection system is an important aspect of security patrol that is too often overlooked by patrol officers. All aspects of the trash collection system should be constantly inspected. Trash carts are a common means of moving stolen or contraband material.

## Importance of the First Patrol Round

The officer's first patrol check of an assigned area is extremely important. During this round, the status of the patrol area is determined. The first patrol thus provides a basis for comparing all subsequent patrol activity. Professional security officers carefully check their assigned areas to determine whether the necessary doors are locked, whether lights are on or off, and whether fencing is intact. They note general conditions, such as the number of people in an area that may require individual assistance or extra surveillance, and special conditions, such as areas that create different safety hazards. Patrol checks on the second and subsequent rounds are geared to observe any changes in the environment. These changes signal conditions to be evaluated to determine whether security has been breached or whether there is cause for action. A standard operating procedure is to vary rounds so that they do not occur on a recognizable schedule.

It is important to recognize that every security officer patrols with a unique point of view based on his or her background and previous experience. Some officers are persistent door checkers but observe little detail while on rounds. Others are less inclined to spend much time checking locked areas, but take careful note of all people encountered on their rounds. Some officers check out-of-the-way places more frequently than others. All officers tend to establish a pattern by which they alertly patrol their areas.

Security administrators take advantage of this knowledge by frequently rotating personnel and changing their assigned patrol areas. These changes can occur during a shift or at periodic shift assignments. If possible, changes in assignment should occur during shifts to provide the best possible patrol coverage and to avoid security officers, becoming bored.

Not all patrol is generalized and random. There will always be a need for certain intensified inspection of a closed area or of an area that has been the object of security problems. An example would be a parking lot that has experienced many breaking and entering incidents. This theory of patrol variation might also be called a selective or concentrated patrol. It is the same concept that traffic enforcement agencies have used to assign extra patrol coverage to areas subject to a high number of accidents or violations.

## Reporting for Duty

Officers reporting for work must properly prepare themselves to effectively provide security service during their tour of duty. Some programs schedule a 15- or 30-minute overlap of security officers during shift changes to allow incoming and outgoing security personnel to exchange information. Unfortunately, in actual practice, most of this time is used for socialization. The result is a waste of labor both in terms of coverage and economics.

Incoming officers can quickly prepare for duty by reviewing the activity (including incident and condition reports) that has occurred since their last tour of duty and by reading any information entered in the pass-on book or electronic briefing systems. Incoming officers should relieve officers going off duty in the field rather than in the office. Any necessary discussion or exchange of equipment can be accomplished in the field without losing field patrol time.



In large security programs where several officers report for duty at a specific time, a formal incoming officer-briefing period can be performed. Essentially the same material is disseminated as when a single officer reports; however, it is presented by a briefing officer. This briefing period can also be effectively used for training. A short period devoted each day to training is an extremely effective method of instruction.

In recent years, the US Department of Labor has targeted the security industry for pay practice violations. In particular, the length of shift change has been targeted. The healthcare security administrator is strongly encouraged to coordinate and review all shift change practices with their human resources department to determine if the length of extra time (if any) is considered *de minimus*.

## Shift Rotation

Security personnel are subject to all human frailties, including complacency and boredom. When one performs the same activity every day, one tends to develop a routine. Even though security personnel are called on to perform many varied activities during a shift, the basic work is routine and subject to patterned activity.

Just as important as the rotation of work assignments during a shift is the periodic rotation of shift assignment. Security officers must be knowledgeable about the security duties and the general activities of every shift to provide optimum protection services. In other words, each officer must be exposed to the total protection system and environment. The protection effort changes hour-by-hour and shift-by-shift in all organizations.

Systems that rotate security officers between different shifts and facilities automatically provide new and challenging situations. Security officers faced with a change in environment, including new people and activities, generally provide a higher level of protection. Officers who are not completely at home with this new challenge will read directions in more detail, ask more questions, be more objective in dealing with staff with whom they have not had time to develop friendships (or animosities), and follow directions in more detail. Officers who are rotated to new shift assignments often discover security deficiencies or initiate improvements not perceived by their predecessors.

One of the strongest objections against rotating shift assignments is that officers do not get to know who belongs and who does not belong in the facility or in a particular area. This argument has only limited validity; it is often personal relationships among employees and others that provide a strong rationalization for shift rotation. The overly friendly or adverse relationships that have evolved are mitigated or terminated, at least for a time.

Security officers can usually determine whether or not a person belongs by checking with known personnel or by simply making a positive inquiry or contact with the individual.

How often should personnel be rotated? There is no established timeframe; however, a cycle of 6 months to 1 year works well. Too-frequent rotation does not give officers adequate time to adjust their personal lives.

Rotating all the security personnel on one shift at the same time is also not advisable. Security officers should work with other officers who have been on the shift for some

time, thus rendering a continuity of service. Officers should be rotated individually. Some officers need to be rotated quite frequently, and others can remain quite objective for a long period of time.

The individual rotation plan also allows officers to work with different security supervisors, which provides two benefits. First, officers are exposed to more in-depth supervision and development because each supervisor has a different point of view and a different method of leadership. Second, supervisors are stimulated to some degree by assuming responsibility for new officers. In explaining the system and procedures to a new officer, the supervisor also benefits by program review. As a general rule, supervisors should be rotated less frequently than security officers. The shift supervisor is considered the thread of continuity for the program.

## Patrol Verification

In all programs it is necessary to supervise patrol officers to learn whether objectives and standards are met. The best method of patrol verification is the field supervisor, supplemented by secondary methods. In small programs, no direct field supervision may be available, and thus secondary methods are used to verify patrols. One such method is the mechanical watch-clock, which has been in use for many years and has largely disappeared from most programs. However, with this system, checking in at the clock station can become the officer's primary objective, with little observation or inspection activity occurring between clock stations. Another problem encountered with the watch-clock system is the clock itself. When security officers are already laden down with equipment, the clock can become quite burdensome.

Some programs have overcome this problem by installing electronic reporting stations. Officers carry a key or other means of signaling the designated reporting station rather than a clock. The signal is transmitted to either a proprietary monitoring point or to a commercial monitoring station. The officer must normally report at each station within a certain time. If the signal is not received within the required time, the dispatcher or monitor initiates a field check to find out why the officer failed to report.

Electronic tour-reporting systems are also being used increasingly. Several companies manufacture this equipment, which reads bar codes or magnetic strips located throughout the patrol area. The officer carries a small handheld computer that reads "the point." Most systems also permit officers to enter data into the computer during patrol rounds. At the end of the shift or at some other designated time, the computer is placed into a charger, which also downloads the data and prints it on a personal computer.

Another type of patrol verification system is an adaptation of the electronic access control system. This system permits each facility's electronic access control system to become a reporting system. This approach entails the security officer presenting their issued identification badge to the card readers in the facility as they go by during each patrol. Through administrative user reporting, the information can be downloaded to a spreadsheet for analysis and documentation purposes. An obvious benefit of this system

is that officers do not have to carry any additional equipment and the organization does not have to install or maintain special readers throughout the facility.

### The Patrol Officer's Key Ring

Patrol officers must carry certain keys to effectively carry out their responsibilities and to provide necessary services. Officers do not need to carry keys that grant access to every locked door within the facility. Conventional wisdom holds that officers must be able to gain instant access to any area in the case of fire, but professional security administrators distinguish between total access and an overly restrictive access policy. Security personnel are subject to error and human weakness and should not unduly be put in a position of temptation or suspicion. Just as security administrators strive to reduce the opportunity for incidents in general, they must also protect the security officers and the integrity of the protection program.

Each locked area of the facility must be evaluated and a plan developed regarding access requirements. For example, consider the need for security officers to carry a key to the general storeroom. (Note the term *carry*; access to a specific key for a particular area is not at issue here.) The general storeroom is particularly vulnerable to pilferage and theft. Most storerooms are protected against fire by sprinkler systems, or at least by an automatic fire detection system, negating the need for a security officer to conduct periodic internal fire inspections. If a fire alarm were activated in this area, the security officer would likely have sufficient time to obtain the necessary key before the fire department arrived. If necessary, the fire department could enter forcibly, which is acceptable compared with the risk incurred by officers who carry keys to be used "just in case."

Various methods allow access to areas without compromising control. In small facilities such as nursing homes, and even for certain areas in large facilities, the double-lock system is quite effective. This system requires two people, with two separate keys, to gain access through a particular door. This solution was effectively applied to a maintenance storeroom in a facility that had experienced a loss of electrical and plumbing supplies attributed to the maintenance personnel themselves. The maintenance personnel obviously needed access to this area. Each maintenance person now carries a key to one lock and the security officer carries a key to the second lock. The double lock prevents either person from gaining entry to the storeroom without the other.

Another simple way to eliminate the need to carry a key is to make the key available at a location controlled by another department. The key can be released to certain predetermined employees after a record is noted that includes the name of the person receiving the key and the date and time of checkout. A common holding area is the switchboard room, the cashier area, or a central security office in larger operations. Collusion between employees can always result in a compromise; however, the probability of this occurring is quite low.

A key management system currently in use at Northwestern Memorial Hospital in Chicago appears to handle the access problem very effectively. The keys to all areas are maintained in the central security office, which is operated 24 hours per day. There is an

electronic key vault for storage of each key in the facility. Critical keys, such as for the gift shop, pharmacy, cashier, and storage areas, require card access and a personal identification number (PIN) to access a certain key. This system electronically catalogs and tracks the key used, by whom, and when.

## Security Officer Response

Security officers on patrol are the first to respond to calls for service and will most likely encounter situations that require intervention, from simple inquiry to the use of physical force. The healthcare setting presents many situations requiring response to routine calls for assistance, response to crisis situations, and critical incident response.

Routine calls to provide an escort, to unlock a door, or to assist a motorist require an efficient—that is, timely and knowledgeable—response. The term *timely* should need no explanation, but officers often give these calls low priority. To the department and the person seeking assistance, they are no less important than emergency calls. Thus, all routine patrols should be suspended and the officer should proceed where required as quickly as possible. Knowledgeable response means not only having enough information to complete the task, but having the proper equipment. For example, officers should know every key on their key ring, including which locks require special procedures.

Response to a crisis situation demands extra preparation and an adequate skill level. *Crisis* has been defined as a significant emotional event or a radical change in one's life that has reached a critical stage. Proper security intervention requires a working knowledge of basic de-escalation principles, including verbal communication, nonverbal communication, personal space, and territory.

Officers also must know what to say and how to say it. Words are important, and the tone and volume of voice can also carry different meanings. A fast rate of speech may convey that the officer is afraid, uneasy, or lacks confidence. Tone can indicate such messages as anger, resentment, assurance, and attitude.

Nonverbal communication consists of posture, eye contact, facial expressions, hand gestures, and appearance. Everyone uses body language and must be aware of the messages being sent. Body language can convey comfort, concern, sympathy, hate, disrespect, disbelief, authority, and confidence, among other things. Security officers need to practice positive body language as part of their training, not only for handling crisis situations but also everyday personal interactions.

The issues of personal space and territory are closely related. Space is generally related to physical area, and territory is related to environment, such as the workplace and home. Security officers generally work more with the aspects of space. In general, personal space is the area around the individual that others are expected not to invade. This area is different for different individuals and is affected by personal traits, habits, environmental factors, culture, and gender. Although it is hard to be specific, personal space can range from 18 to 20 inches for intimate contact, and 4 to 5 feet for public contact. Intruding in this space can escalate a crisis. This does not mean that security officers

cannot enter this space to resolve a situation. It merely means that they must be aware of the concept and the ramifications of their actions.<sup>5</sup> The rule of treating others as you would like to be treated is prudent and practical in all situations.

Security officers responding to a critical incident should follow these guidelines:

- Upon receiving notification, proceed quickly and safely to the scene. Do not run. Arrive in a composed manner, cautiously proceeding into the area.
- Perform a quick assessment, gather basic information, and determine an initial course of action.
- Alert other appropriate resource personnel (dispatcher, additional security personnel, police, fire, etc.) with succinct and pertinent facts.
- Direct action at the scene. Minimize danger to yourself or others and limit further damage if possible.
- Secure the scene, identify witnesses, and preserve evidence.
- Take notes, obtain statements, and complete an incident report.

## Patrol Problems

Several common problems involving patrol officers in medical care settings require close supervision and repetitive training, regardless of how basic these problems appear on the surface.

The first major concern is excessive socialization. Since many security personnel are male and most healthcare personnel are female, frequent socialization is an inherent problem. It is true that it takes two to socialize and that the problem involves both employees; however, the nonsecurity employees are generally in their assigned work area. When officers linger too long in a particular department, they are not only neglecting their duty, but also hindering others from doing their job.

A second major problem is the tendency of security officers to talk too much. This tendency relates in part to the previous issue; however, the main concern is discussing confidential security information with nondepartment personnel. One hospital administrator reported receiving more security information from the telephone operator being briefed by security staff than directly from the security department itself. Security officers should not be overly secretive, but they should discuss security plans, programs, and problems only with appropriate persons.

When looking for a security officer, some persons automatically check in the coffee shop or cafeteria. Security personnel gravitate toward these locations and consequently spend too much time there. Uniformed officers sometimes go to the cafeteria or coffee shop before or after their tour of duty. The problem is that the officers are the only ones who know that they are off duty. To others, the officers appear to be on duty and wasting time.

Perhaps the biggest problem in patrol deployment involves keeping officers separated when more than one is on duty. Of course, officers should back one another up on a call and give other legitimate assistance, but they should not congregate simply to pass

the time. When more than one officer is on duty at a time, it generally means there is too much area or work load for one officer to perform adequately. When two officers are together, the effective coverage is reduced to that of a single officer. Healthcare administrators frequently cite this issue as one of their largest frustrations with the security department.

Reading while on post is most prevalent in fixed-post assignments. This situation reflects rather poorly on the entire security effort. Reading should be limited to material pertaining to the job and supplied by the program and should never interfere with job performance.

Although these concerns cannot be considered to be in-depth supervisory problems, they are real, and they occur in all security systems to some extent. Such minor problems have had a significant impact on keeping security officers in the low-status position that they are to a great extent trying to rise above.

## References

1. Kent Hospital. (2006, October 23). Kent adds new security bicycle patrol. Retrieved April 30, 2009, from <http://www.kenthospital.org/body.cfm?id=84&action=detail&ref=81>.
2. Carolinas healthcare system deploys segway PT i2 police packages on its campus. (2007, November 11). *SecurityPark.net*. Retrieved November 22, 2007 from [http://www.securitypark.co.uk/security\\_article260108.html](http://www.securitypark.co.uk/security_article260108.html).
3. MacDonald, C. (2007). Vehicle alternative stands out from a crowd. *Campus Safety Magazine*. Retrieved April 29, 2009, from <http://www.campussafetymagazine.com/Articles/?ArticleID=108>.
4. Slogowski, J. (2008, October 10). Dogs add bite to security at hospital. Retrieved October 12, 2008, from <http://www.yourwestvalley.com/common/php?db=dnsun&id=4007.html>.
5. Church, W. C. (1989, March). Keeping crises cool. *Security Management*, 143–146.

# Program Documentation

The preparation and maintenance of security records and reports can be extremely time-consuming for line and administrative staff. Unnecessary records and reports take away valuable time that could be spent performing meaningful incident prevention, investigative duties, and general security services. An objective of the security documentation system should be to maintain only the records and reports that are truly necessary and to improve the efficiency and quality of the documentation system. It is acknowledged that a basic component of the successful security program is a comprehensive and useful documentation system. However, documentation that is simply maintained, for which there is little or no use, simply wastes valuable department resources. Author Barbara Hemphill in her book *Simplify Your Workday* states that 80% of the paper (records) we keep is never referred to again.<sup>1</sup> The term *documentation* includes budget and fiscal documents, personnel records, policies, procedures, correspondence, bylaws, contracts, reports, and a whole host of specific records. This chapter is limited to the discussion of operational records and reports utilized in a healthcare security program.

## Purpose of Records

The use of, and necessity for, specific security records varies from organization to organization; however, the primary reasons to maintain records are basically the same for all organizations. Records provide a memory system, permit the exchange of information, direct operational procedures, fulfill various administrative needs, and assist in the verification of security activity and general planning processes. Within each of these primary reasons are many subcategories designed to provide operational efficiency and effectiveness for the healthcare protection system.

## Memory System

The need to retrieve information contained in a report may occur within hours, days, or even years after it was completed. A quick and effective technique for evaluating a security system is to determine how many questions concerning past incidents or activities are answered by personal memory and how many questions are answered by documented facts.

One of the inherent problems of security operations is that it is difficult to anticipate today what information contained in records and reports will be required tomorrow. It is

not only major incidents, but also the so-called minor incidents for which information is later required for various reasons. Although the statute of limitations for litigation proceedings varies from state to state, all are measured in years rather than months. Lawsuits are sometimes filed at the last minute in the expectation that supporting defense information will be lost, forgotten, or incorrectly interpreted due to the time lapse.

Not only do civil lawsuits illustrate the need to preserve facts, but also the overloaded criminal justice system may require certain records and reports years after the actual event. The term *continuance* is often heard in criminal actions. Delay after delay can result in a considerable period between the time the action was initiated and the time adjudication is completed.

The use of recorded facts as a memory system is a major aspect of the investigative function. Records are as important to the investigator as scalpel is to the surgeon. Trends, modus operandi, and the facts of past incidents can be instrumental in successfully concluding an investigation.

## Exchange of Information

The exchange of certain security information is required among members of the security department, organizational management, and various outside agencies. The interchange of information among security personnel allows the security staff to be knowledgeable of the profile and events of the environment they are protecting and serving. This information is necessary for each officer to effectively carry out his or her responsibility. Security protection could be increased by perhaps 100% if all the bits of information known by all members of the security force could be assembled and organized in a meaningful manner. While some exchange of security information is verbally transmitted the vast amount of such information is exchanged via some type of report.

Reports are necessary to record questionable activities and security deficiencies in order that they may be transmitted to an appropriate person or department for follow-up action. General security information that affects an organization must be effectively conveyed through the appropriate channels.

Information transmitted to local, state, and federal law enforcement agencies has often supplied the link that allowed the agency to successfully conclude an investigation. Progressive law enforcement administrators and professional security administrators establish working relationships that recognize positive contributions that each can render to the other. Security information transmitted outside the organization also includes insurance companies, planning agencies, fire departments, offices of emergency preparedness, and other similar organizations.

## Operational Policy and Procedure

Security operations require policies and procedures to direct the proper delivery of emergency and routine security services and actions. Operational security policy and procedures are most often referred to as *post orders* or *facility orders*. A goal of security



operations is to achieve professional and consistent actions by all the security staff in the discharge of their daily responsibilities.

The terms *policy* and *procedure*, along with the term *protocol*, are often used interchangeably. They are in fact somewhat different, but very closely linked together. For the purposes of this text, these terms are defined as follows:

- *Policy*: A stated objective and/or stated principle.
- *Procedure*: A manner of proceeding, way of performing, or a series of steps to be taken to comply with policy.
- *Protocol*: A code of conduct and/or a plan for the course of treatment used more often as a medical term.

One should always be cognizant that not all policies and procedures are created equal. Some will need to be general in nature and some will be quite specific. As an example, the security response to a critical incident may be somewhat general in terms of steps and the exact sequence of those steps. On the other hand, the collection, storage, and release of patients' valuables will need to be quite specific in the series of steps required.

#### *Problem Areas to Be Avoided*

There are various pitfalls that, when avoided, make the job of maintaining good policies and procedures easier and more user-friendly.

- Avoid the commingling (mixing) of policy, procedure, and training/educational information. Too often the writer feels compelled to add rationalization (the why), or educational information, which tends to result in a convoluted procedure without a crisp clarity.
- Always do a search for other organization policy and procedure on the same subject to ensure that security policy and procedure are compatible and in accord with the organization. When the new, or existing, security directive is or will be in conflict with other directives, take a time out. Contact the author, or administrative person responsible, to arrange a discussion regarding fixing the conflict of information.
- Correct any policy that may have changed, or a written procedure that does not coincide with the actual practice. This discrepancy may be corrected by changing the policy and procedure or result in training of field staff. It may also mean enforcing staff compliance.
- Check that policy and procedure reflect the general healthcare security industry standard practices. There may be a reason that it falls outside of the standard practice, which may be okay, but be ready to defend the position. An example of a policy that shows up every now and then is: "Security officers are not allowed to touch patients." This policy is clearly outside of the healthcare industry security practice and the standard of care. Defense of this policy may be difficult, but is most likely to be challenged at some point along the way.

- Minimize word count. Organize procedure in step-by-step directive when possible. Use short sentences or phrases.
- Combine new policy and procedure with existing one when possible.

Policies and procedures should be working documents and updated as needed. All policies and procedures should be reviewed (evaluated) annually and redated even if there are no changes. A security review committee of three persons should formally examine each policy and procedure. As a consideration, this review committee could be the Director or Manager of Security, a Security Supervisor, and a Security Line Officer.

## Administrative Records

Security records fill many needs in the administrative control and effective operation of the protection program. Although each security department requires specific records peculiar to its own operation, certain administrative records are needed by all operations, regardless of size, to provide a viable and accountable service.

One of the basic uses of records is the location and identification of security needs through the statistical analysis of recorded security information. Once a need has been identified, and a possible solution devised, the technique for measuring the effectiveness of the solution is the ongoing analysis of the same security records that first identified the need. In addition to identifying problems, security records are useful in projecting trends. Early awareness of a possible security problem allows preventive measures to be implemented.

The deployment of security force personnel is predicated on existing or projected security needs. On the basis of records, security administrators can objectively deploy security personnel at the times and in the places that are most effective.

Security officers for the most part perform their duties without being directly observed by a supervisor. A security officer's evaluation must, to some degree, include a comparison of individual activity with that of other members of the security department. Record list assignments, assign responsibility, and verify the accomplishment of tasks. Adequate records measure an officer's relative capacity for work and indicate special abilities and aptitudes, as well as areas of work performance requiring improvement.

Department records are necessary to account for security property and to ensure the proper functioning and maintenance of equipment. Preventive maintenance and timely repair of security equipment reflect well on the quality of department leadership. A history of maintenance and repairs is essential to justify equipment modifications and strategic planning of equipment replacement.

## Documentation Policy

Documentation systems should be implemented and controlled according to detailed organizational policy. Norman Bates, President of Liability Consultants, Inc., suggests

a five-point document policy which includes presentation, content, correction, review, and retention.<sup>2</sup>

- *Presentation:* The report conveys a nonverbal image to the reader. The visual appearance of the report provides the opportunity to present a professional image.
- *Content:* The report should be clear and comprehensive to the point that it is understood by a reader unfamiliar with the event or situation.
- *Corrections:* A review of a report by a supervisor or manager can find errors including spelling, grammar, or structured deficiencies. The original author should make the necessary changes, which may require that the report be rewritten.
- *Review:* Document review is an essential tool in proper program management. Information obtained from document reviews is the basis for program planning, assessment of training needs, initiation of disciplinary actions, supporting litigation considerations, and measuring activity.
- *Retention:* In terms of litigation, documents may either subject the organization to liability or protect it from liability. A document retention policy should ensure that documents are retained at least through the time frame of the statute of limitations for negligence and any legislation that exists.

## Report Formats

The format/style of security reports is one of individual preference, but must be designed in a manner that assists the report writer in preparing a complete report in an efficient manner. Electronic report preparation may, or may not, meet this expectation.

Whenever a new report form, or the updating of a current form, is considered, the security administrator should ascertain that the form is absolutely necessary. The next consideration is simplicity. Needless records and reports that are overly complicated make paperwork tedious and time-consuming, all of which can result in reluctance on the part of security officers to complete their reports. The excessive time required to complete the form reduces valuable time in the field. Regardless of the format, the guiding principles for all types of reports should be accuracy, simplicity, and efficiency.

Security reports come in all sizes, shapes, colors, and designs. The design of report formats falls into three basic classifications:

- Narrative style
- Check-off or block style
- A combination of narrative and check-off styles

These three types of formats have certain advantages and disadvantages; however, the combination style is the format in predominant use.

### *Narrative Form*

The narrative style can be used for the creation of virtually any type of security report. It is the least expensive of all styles. Stocking and supplying the form is logistically uncomplicated.

The basic disadvantage of the narrative form is that it requires a higher level of training than other types of reports. The preparation of a narrative form can also be very time-consuming.

#### *Check-Off Form*

In contrast to the narrative form, very little training is required to complete the check-off form because all the necessary information is shown on the form. The check-off form is highly specialized and is the most expensive type of form to create. A basic advantage, especially in electronic form, is the ease of extracting information categories for the who, what, why, when elements of trending and data evaluation.

The high cost is largely due to the check-off format, when hard copy reporting forms require many different forms to cover different types of incidents. It can be difficult to have the proper form in the field when needed to guide the collection of information. A common problem with check-off forms is that more than one page is often necessary because so many alternatives must be listed for each question.

#### *Combination Forms*

Since the nature of security incidents in the healthcare setting is so widely varied, the most popular and the most functional type of reporting form is the combination report, a form that uses both narrative and check-off formats. The combination report can be used for virtually any situation that requires a report.

#### *Other Format Considerations*

In addition to report format design, other considerations include color coding, number of copies required, and size. Two systems for color-coding reports are popular. The first is to color code by type of report and the second is to color code for distribution or filing. The latter is the most common approach. The number of copies required for a specific report is determined by the organization's structure and needs.

In hard copy systems, the use of no-carbon-required (NCR) paper has many advantages when multiple copies are required. When preparing a report printed on NCR paper, one must take care to separate the sets of forms from the supply before writing. A single-sheet draft form for officers to outline their reports is worth considering. Even the best report writers begin a report and for one reason or another must start over. A single-copy draft report identical to the multiple-copy NCR form will save money. Some forms can be printed on both sides of the paper to save money. This logical approach is often overlooked. Forms that lend themselves to this practice include logs, activity sheets, maintenance records, and other single-sheet records.

## Computer-Generated Reports

Computer-generated report preparation may eliminate the need for hard copy forms. Generating report copies becomes a much simpler administrative procedure as the electronic report is simply created, stored, and reviewed on the computer. Printed copies

are generated only as needed. The computer-generated reports require a series of controls. A simple password protection is not very secure; however, more complex mechanisms involving tokens (magnetic, RFID technology, biometrics, and others) have their own drawbacks. Computer security always involves trading security for ease of use. A disconnected computer locked in a vault is still dependent upon the security of that vault. In order that originally generated documents cannot be changed, a form of version control must be instituted. In a version control system, the original stored document is never altered. Authorized users (i.e., supervisors) may “check out” a copy, make changes, and enter their altered version. In this system, the original is saved and any revised versions are time-stamped and logged in the user who submitted a new version. A pitfall to be avoided in digital storage of documents is that all copies are perfect copies, and these changes may be undetectable without an unaltered copy of the original document for comparison. It can be said that a document signed by the originator is still a good process in maintaining the integrity of the document system.

A serious operational pitfall of report preparation is lost field activity time of the security officer(s). It is common for officer(s) to perform their report preparation in the quiet of the security office, often located in an out-of-the-way location. A problem that has been consistent over time is how to keep officers out of the office and in the field, especially on the late afternoon, night, and weekend shifts. The practice of computer-generated reporting can actually promote excessive office time by providing an excuse for being in the office, relaxing and socializing. A good management practice, whether report preparation is accomplished as a hard copy, handwritten system, or computer generated is to establish several field locations where the officer completes reports. The key to maintaining officer field activity is to locate these report-writing stations where the officer can observe a public/staff area and be available for questions or requesting of services. The field report writing may be at the front lobby desk, open admissions desk, or a regular security fixed post. In utilizing a security fixed-post computer terminal, the officer at the fixed post simply trades assignments with the officer needing to complete a report. The regular fixed-post officer thus can go on patrol and the officer completing his report assumes the duties of the fixed post. When the report is completed, the two officers return to their original assignments.

## Basic Records

Basic administrative and operational records must be maintained in all healthcare security systems. Administrative records include employee time records and pay records, management reports, property accountability records, employment and training records, lost and found logs, dispatch/alarm logs, visitor logs, statistical analyses, vehicle registration records, key control card access records, and the like. The most important operational records are security incident reports (SIRs) (including supplemental reports), security condition reports, daily activity reports, dispatch logs, property accountability, and various vehicle reports and records. Individual security programs will have requirements for records and reports unique to their specific program.

## Security Incident Report

The basic record found in all security operations is the security incident report (SIR). This report should not be confused with the unusual incident report (UIR) that is commonly utilized by clinical staff to report medication errors, patient falls, and other clinically related situations. These two types of incident reports (SIR and UIR) should be maintained separately and not combined into a single multiuse form. In some systems the SIR is known as a *case report*, an *offense report*, or an *investigative report*. These terms are basic police nomenclature and should be avoided. A widely accepted but general definition of a security incident is any security-related situation not consistent with the routine of normal operating procedures or conditions. An example of a SIR form is shown in [Figure 11-1](#).

The IAHS Basic Guideline on Security Incident Reporting provides a foundation for planning and developing the incident reporting system.

### IAHSS—HEALTHCARE BASIC GUIDELINE, #05.01

#### **Security Incident Reporting**

**STATEMENT:** Healthcare facilities (HCFs) will develop procedures for reporting and documenting security incidents. Reports serve many purposes including sharing of information in a timely fashion and compiling facts and circumstances for later review.

#### **INTENT:**

- a. Alleged crimes; emergency responses; incidents involving injury, loss, or damage; and physical interventions that come to the security's attention should be documented as soon as possible.
- b. Documentation should be in written form: either in hard copy or electronic format. If electronic, data backup and recovery procedures should be developed and periodically tested.
- c. Report forms should be formatted to assist in gathering pertinent information and in compiling trends and comparisons.
- d. Statistical trends should be regularly reviewed for the purpose of taking proactive action as indicated. (See IAHS Guideline 06.01, intent e.)
- e. Follow-up reports, referencing initial reports, should be filed indicating additional notifications made, additional information received, and additional actions taken.
- f. Reports will sometimes contain mere allegations and other personal data that are inappropriate for dissemination into the public domain. As such, each HCF should develop procedures setting out when and how reports may be released.
- g. The report system should include a written report retention policy in keeping with the HCF's overall document retention policy.

#### **REFERENCES/GENERAL INFORMATION:**

- IAHS Guideline 06.01, General Program Measurement/Improvement.

**Approved:** December 2006

**Last Revised:** October 2008



### *Security Incident Statistics*

The SIR, in aggregate, is the primary source of data which identify past security incidents or situations occurring at a facility or within a hospital system. The most common method of presenting this information is via statistical reporting of the number of incidents, by incident category, for a specific time period in a spreadsheet format. This type of statistical reporting is sometimes referred to as a *snapshot* of past incidents. It is suggested that this statistical report reveal numbers of incidents in blocks of combined categories. The defined categories would be created by the hospital security administrator in concert with the chair of the Environment of Care (Safety) Committee. A starting point could be to review the security risks as outlined in *Chapter 3, Security Risks and Vulnerabilities*, Figure 3-1 of this text, and combine certain risks into a single category. The purpose of the categories, as opposed to utilizing each single risk listed, is to render the report more manageable and eliminate presenting a report with a preponderance of zeroes. In addition to the risk category type there could be additional categories such as “Information Only” Incident Reports, Alarms, Found Property, etc. [Figure 11-2](#) is an example of the Security Incident Statistical Report.

### *SIR Considerations*

Every healthcare security program must define the parameters or conditions that require an incident report. There are gray areas to be sure, and the reporting of every incident is virtually impossible. When officers conclude the handling of a minor incident, they tend to avoid preparing a report. In addition, different security programs have different reporting procedures for minor incidents. For example, suppose a security department receives a report that a patient is missing a ring, but when the security officer arrives, he is advised that the ring was found in the narcotics drawer. In some programs the officer would not be required to report such an incident; in others he would simply note the incident in the daily activity log; and in other programs an incident report would be required. The daily activity log is preferred as the most efficient approach. One program defines the necessity of completing an incident report in terms of the number of sentences required to record the event. In that program if the occurrence has been successfully concluded and can be described in three sentences or less, the information is recorded in the officer’s daily activity log, and no incident report is completed.

The basic rule is, “When in doubt, write it out.” In other words, if an officer is uncertain whether an event should be reported, an incident or other specialized report should be completed.

Progressive security officers develop skills in observation and investigation, which are two of their needed primary security skills. However, it is not enough to develop these skills unless the results can be recorded accurately, clearly, and succinctly in the preparation of the subsequent incident report.

Even seasoned officers find report preparation one of the most difficult parts of the incident investigation and reporting process, and the most difficult part of reporting is



**UNION HOSPITAL  
SECURITY INCIDENT/INFORMATION REPORT  
2009**

	J	F	M	A	M	J	J	A	S	O	N	D		
Category													This Year Total	Previous Year Total
Alarm-Security	12	8	9	4	6	6								<b>87</b>
Alarm-Fire	3	1	2	0	3	2								<b>23</b>
Assault	0	1	0	0	1	0								<b>2</b>
B & E	0	0	0	0	0	0								<b>1</b>
Disturbance	2	3	3	2	4	6								<b>37</b>
Elopement	0	0	0	1	0	0								<b>3</b>
Fires	0	1	2	0	0	0								<b>5</b>
Missing Property														
-Hospital		4	7	4	8	6								<b>58</b>
-Patient	7	5	3	3	4	3								<b>51</b>
-Staff	2	3	3	2	0	1								<b>18</b>
-Visitor	1	1	2	0	0	2								<b>9</b>
-Vehicles	0	1	0	0	0	0								<b>3</b>
Patient Assist	14	16	14	18	12	19								<b>191</b>
Robbery	0	0	0	0	0	0								<b>0</b>
Stalking	2	0	0	0	1	0								<b>4</b>
Threats	4	5	6	5	5	4								<b>53</b>
Vandalism	1	0	2	1	1	2								<b>17</b>
Information Only	8	11	11	14	10	12								<b>109</b>
<b>Total</b>	<b>62</b>	<b>60</b>	<b>64</b>	<b>54</b>	<b>55</b>	<b>63</b>								<b>671</b>

**FIGURE 11-2** An example of a security incident statistical report.

often the beginning. The key to completing an incident report is to record information in a logical sequence. If the report is written in a logical sequence and the writer has adequately answered the basic interrogatives (who, what, when, where, and how), and the actions taken, the report will be essentially complete.

A report must be objective and must include both favorable and unfavorable facts. If a report contains an estimate, such as distance or size, it should be identified as such. Personal opinion should generally not be included in reports; however, an opinion can often be valuable in evaluating the facts. It is not necessarily wrong to include an opinion if it is clearly identified as such with some supporting rationale. For example, an officer who reports information from someone who seems vague, inconsistent, or contradictory may wish to note that the person did not appear completely rational and might have been under the influence of drugs or might be suffering from a form of dementia. However, it is generally accepted that opinions or suppositions be recorded on a separate sheet of paper and attached to the formal report.

In some security departments, handwritten field reports are later typed by a department clerk. This is a poor practice for a variety of reasons, not the least of which is cost. Many departments have transitioned to electronic security incident reporting software programs. Although officers require more training and practice to complete these computer-generated reports, report writing quality and appearance have both been shown to significantly improve while spelling errors and illegibility have all but been eliminated. To date, the average time to generate an electronic report continues to take longer to complete than the traditional handwritten report. This trend is expected to reverse as the population in general continues to grow more accustomed to computer technology. In addition to the advantages noted above, many off-the-shelf incident reporting and investigation management software packages offer a clear authority matrix approval process before a report is released and sophisticated analysis, statistical reports, and predictive modeling capability.

Security officers should not be allowed to go off duty before completing their required reports. Reports should be completed as soon as possible after the facts are collected. In the cases where a security officer initiates an investigation just before going off duty, the incoming officer can assume responsibility and relieve the first officer. Incident reports can be initiated by one officer and completed by another. The report must identify where the relieving officer took over; this can be simply stated in the body of the report.

The administrative review of field reports has several distinct purposes. One is to provide feedback to the officer who prepared the report with constructive comments on how the writer could have prepared a better report. This task is an example of how training and supervision are interrelated. We all learn through our mistakes; however, no learning takes place if our mistakes are ignored and we are not made aware that a mistake, error, or substandard performance has occurred.

The administrative review also ensures the completeness of the report. Officers should be encouraged to prepare a rough outline of the report to make certain that they have the proper information organized in good form before they begin to write. This method helps eliminate false starts and reduces the waste of costly multiple-copy forms.

## Security Supplemental Report

The supplemental report form is used to record additional information to the original report. Supplemental reports are generally used in conjunction with SIRs, but they may also be used as a follow-up to other records or reports. Commonly this form is used to record follow-up investigative information. For example, after reporting a case of missing property, a security officer will often discover that the property was recovered. If the original report has not been distributed, the facts can be added to the original report indicating the new time and date of the information being added. However, if the original report has been distributed, a supplemental report is prepared to be matched to the original loss report at a later time. Also, it is common practice to use supplemental report forms if additional pages are required when preparing an incident report. [Figure 11-3](#) is an example of a security incident supplemental report.

Once an incident report has been completed and distributed through administrative channels for information, recording, or follow-up, the report must be filed so that it can be efficiently retrieved. One of the simplest methods of filing hard copy incident reports is by date. Only in very large security departments is it necessary to use a system of serial numbers. In some departments, copies of the incident report are filed as cross-references. This system tends to create more paperwork than necessary. Electronic systems permit a vast number of references and reports to be searched in many ways.

## Security Condition Report

The security condition report is a report used to advise others in the organization of a security condition rather than a security incident. It takes the form of a memorandum that describes unsafe conditions, security vulnerabilities, malfunctioning security equipment, areas found unsecured, and other situations that may require action, or should be brought to the attention of others. [Figure 11-4](#) is an example of a Security Condition Report form.

An example of a security condition that should be reported is an office door found unlocked during a late evening security patrol check. Suppose that a security officer is aware that the door is usually locked around 5:00 P.M. and that it had been secure on the last round. Upon internal inspection the office appears to be intact and the security officer assumes that someone who had legitimate access failed to lock the door. A house-keeping, maintenance, or office employee might have inadvertently failed to lock up. However, the possibility that an intruder gained access does exist.

The security condition report serves a couple of purposes in this situation. First, the officer records the date, time, and the action taken, and leaves an information copy of the report in the office to inform the occupants on their return. Their response should then be to determine if anything is missing or if there is any other security problem.

Second, a copy of the report goes to the Director of Security or the person responsible for review for possible follow-up action. This report may fit a pattern that suggests



**S**ECURITY  
**S**ERVICES

**SUPPLEMENTAL  
INCIDENT REPORT**

**SECURITY DEPARTMENT**

Facility: \_\_\_\_\_ Time Reported to Security: \_\_\_\_\_ Date: \_\_\_\_\_

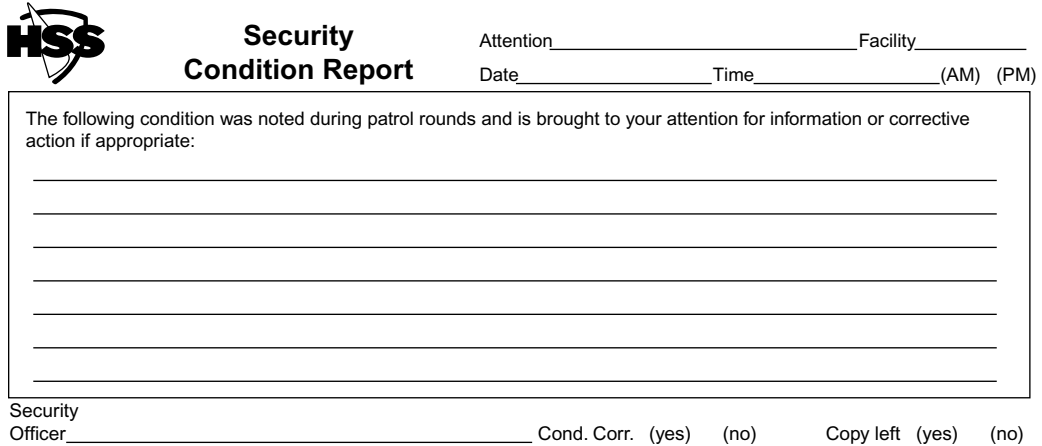
Reported By: \_\_\_\_\_  
Vis Emp Pat | Add/Dept. \_\_\_\_\_ Tel: \_\_\_\_\_

Nature of Incident \_\_\_\_\_ Location \_\_\_\_\_ Time/Date Occurred \_\_\_\_\_

Multiple horizontal lines for writing the incident details.

Security Officer \_\_\_\_\_ Police called at \_\_\_\_\_ Arrived at \_\_\_\_\_ Officer \_\_\_\_\_

**FIGURE 11-3** An example of a security incident supplemental report form (Courtesy of HSS Inc., Denver, CO).



**HSS** **Security Condition Report**

Attention \_\_\_\_\_ Facility \_\_\_\_\_  
 Date \_\_\_\_\_ Time \_\_\_\_\_ (AM) (PM)

The following condition was noted during patrol rounds and is brought to your attention for information or corrective action if appropriate:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Security Officer \_\_\_\_\_ Cond. Corr. (yes) (no) Copy left (yes) (no)

**FIGURE 11-4** An example of a security condition report form (Courtesy of HSS Inc., Denver, CO).

that housekeeping does not always lock up, and a follow-up with the housekeeping department may be indicated.

Another use of the security condition report is to serve as a work order. A copy of the security condition report is sent to the maintenance department, indicating the need for repair or service on a piece of equipment.

Security condition reports can serve to advise other security officers that a condition has been found and reported. For example, officers who note that an officer on the previous shift prepared a condition report about a burned-out parking lot light will not duplicate the report. The condition report thus serves as a communication tool and helps to coordinate the protection effort among officers.

## Daily Activity Report

As a basic rule, all field officers should be required to complete a report of their activities during their tour of duty. There are as many different types (formats) of daily activity reports as there are security departments. [Figure 11-5](#) is an example of a security officer daily activity reporting form.

Examples of entries in the daily activity report include unplanned or unscheduled activities such as escorts, assistance to motorists, release of a body, and miscellaneous information such as the license number of a vehicle that looked out of place, the name of a person not permitted entry to a closed area, or the reasons for not accomplishing scheduled rounds.

The electronic patrol verification system is not a substitute for the Daily Activity Report of the security officer. Total reliance on computer input is not realistic, and all activity reports should allow the officer to add narrative information to the report.

In some larger departments that have a 24-hour central security control center (dispatch), each officer does not complete an individual activity record. Instead, the officer

310 HOSPITAL AND HEALTHCARE SECURITY

SHIFT #8

DAILY ACTIVITY REPORT  
1600-0000

09/08

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_ Officer Name: \_\_\_\_\_

Radio Used: \_\_\_\_\_ Key Ring Used: \_\_\_\_\_ Other Equipment Used: \_\_\_\_\_

TIME ACTIVITY

- 1600 On duty, brief with prior shift, read pass-on, start DAR.  

---

---
- 1615 Check with ED officer and with ED Charge Nurse. Inspect vehicle and complete inspection log.  

---

---
- 1630 Interior check of main hospital. Check Centralized Scheduling, 4th Floor. Assist with calls for service as necessary.  

---

---
- 1700 Check Pharmacy, Central Supply, and Power Plant. Interior check of main hospital. Assist with class for service as necessary.  

---

---
- 1800 Begin relieving officers for dinner breaks as activity permits. Ensure all officers call on and off break on the radio.  

---

---
- 2000 Interior patrol of main hospital.  

---

---
- 2030 Maintain visibility in the main lobby area and the information desk area.  

---

---
- 2200 Check hospital floors.  

---

---
- 2230 Remain near main entrance, outside weather permitting. Assist with calls for service as necessary.  

---

---
- 0000 Brief with oncoming shift, complete DAR, and radio log. Off duty.

I certify I completed all assigned and requested duties as described above.

Signature: \_\_\_\_\_

**FIGURE 11-5** An example of a security officer daily activity report.

assigned to the security control center makes all assignments and directs the activity of individual field officers. A chronological activity log is thus maintained centrally. Entry directly into the computer program is affected at the time of each activity. This system reduces paperwork and makes it much easier to review activity performed by the security department as a whole.

The chronological computer entry record can also be used for various administrative purposes. For example, by recording the time a call was dispatched and the time the officer arrived, a profile of response time can be maintained. Likewise, the time expended on each service activity can be recorded and collated to produce a profile of the time expended for each activity.

One of the pitfalls of the central security control system is that not all requests for service are directed to the security control desk. A good deal of activity is originated by field officers and by direct customer contact with field officers. In these instances officers must notify the dispatch center to initiate the record.

## Parking Violation Notice

The purpose, size, shape, and format of the parking violation notice vary from program to program. The design of the form is obviously dependent on the system of parking control used by the organization. Generally, the violation notice is intended to be a friendly reminder that orderly parking benefits everyone. In parking systems where specific areas are designated for different groups (physicians, visitors, employees, outpatients, etc.), the violation notice takes on a stronger connotation. Some jurisdictions issue citations that include the punitive action of a fine or impound of the vehicle.

The size of the form should be determined to some extent by the uniform or attire worn by security officers. The notices should fit neatly into a pocket or special holder, as patrol officers should carry a supply while on normal patrol duty. The copy of the notice to be placed on the vehicle should be printed on card stock. If additional copies are required, a lighter paper may be used. The form should refrain from having a sticky adhesive quality as it can be a source of unproductive recipient frustration.

## Pass-on Record

Every security department must have a system for transferring information from shift to shift or officer to officer. In some programs this system is known as the “party line.” Various procedures are used to handle this important aspect of security operations. A bound or loose-leaf book is widely used. All officers reporting for duty must be required to read the information added to the book since they were last on duty and to sign each page to signify that they have read the information. The computer is also a useful tool in which the officers coming on duty can simply access this information by logging in to the electronic record.

The information that is recorded on the daily pass-on record originates from many different sources, including administration, department heads, security officers,

and various elements inside and outside the organization. For example, the information entered in a pass-on record might include a vehicle granted special permission to park in a particular area; a new key that has been added to the patrol officer's key ring; a special shipment of products expected during the night, with disposition instructions; the need to block off a certain area of the parking lot for special parking or construction; and a meeting in the facility for which special security activity is required. The pass-on record should include timely information officers need to perform their responsibilities efficiently and effectively. However, the pass-on should not be used to call out employee mistakes or note opportunities for improvement of individual officers.

The security administrator must review all pass-on information periodically to determine if the post orders, policies, or procedures must be modified or deleted. For example, if a key is added to the system, the post order that identifies all keys on a specific key ring and the procedural use of such keys must be updated.

The bound book works well for single-facility organizations; however, for organizations with multiple facilities that are geographically separated, the computer is recommended.

Security administrators should consider including a short training message for each day as part of the daily pass-on record.

## Master Name Index

The master name index is a very simple but extremely useful security methodology. A record is prepared about anyone who has had a significant interaction with a member of the security department or about whom information has been received. The intent is to provide a ready historical reference of individuals through this index.

Names to be included in the master name index are obtained from SIRs, which include names of complainants, victims, suspects, and witnesses. Exactly which names will be included in the index is a matter of individual philosophy. Some departments include names of their security officers, employment applicants, people who have corresponded with the department, and individuals named in newspaper articles concerning the HCF.

The index lends itself to computerization and may be cross-indexed. Small departments without computerization will find the three-by-five index card the most economical approach. The record may simply refer to an incident report, a piece of correspondence, or other records, or it may contain all the information known.

## Monthly or Periodic Security Report

It is common practice to prepare periodic security reports on a monthly, bi-monthly, or quarterly basis. These reports include the monthly security incident statistical report referred to in [Figure 11-2](#). The frequency of the periodic security report is most often the same as the scheduled Environment of Care Committee meetings. In addition to the



statistical incident summary report, the full report may contain such items as status of a security project, summary of the volume of service activities, equipment modifications/upgrades, changes in parking controls, status of performance improvement goals, special events, training activities, and so on. The report will generally be designed for the needs and expectations of the committee.

## Annual Security Management Plan and Program Effectiveness Evaluation

On an annual basis there should be a formal review of the security program which addresses the objectives, scope, performance, and effectiveness of both the security management plan and the operational implementation of the plan. In short, how did the program measure up to expectations? In addition to the security management plan, the periodic reports prepared throughout the year for the multidisciplinary review committee are the basic sources of information for the annual evaluation. The annual evaluation does not need to be on a calendar year basis; however, the calendar year is utilized by most healthcare security administrators. The annual security program effectiveness evaluation continues to be a requirement of TJC.

## Performance Improvement Records

A primary goal of the healthcare security program must be to seek program improvement. Improvement requires setting standards for measuring, monitoring, and establishing improvement goals. Records maintained for these purposes ultimately document program quality. The performance standards vary widely according to program needs. An example is the security alarm system. An alarm system only provides an element of quality when it is operational. A system of periodic documented tests measures the reliability (quality) of the system. Testing may merely indicate whether the system is operating as intended or it may go a step further to measure an operational response to an alarm.

Figure 11-6 lists a number of performance measurements/improvement goals that may be considered for healthcare security programs.

## Keeping Departmental Records Current

In addition to basic records, a protection program may require many different types of records and reports to meet its particular needs. All records and reports used in a security program require a periodic review. All forms should be analyzed to determine if they are necessary and if they are being completed by staff in a satisfactory manner. Do not hesitate to change a form if it does not meet the organization's needs in every detail. The most common error encountered is that forms call for more information than is really necessary. Either time is wasted in obtaining and recording the information or officers tend to ignore certain details.



**FIGURE 11-6** Examples of security performance measurement/improvement.

## Records Retention

The retention of security operational records should be controlled by organization policy, subject to any state law, that ensures that needed records are retained and unneeded records are discarded or destroyed as necessary. As a general rule, most departments retain too many records for too long a time period. Each operational form used by the security department should be assigned a specific retention period. This does not imply that a specific record(s) would not be “pulled out” and saved beyond the stated retention period.

When litigation arises months or years after the actual incident, the plaintiff will generally demand all business records relevant to the claim during the discovery process. The absence of a document retention policy could lead to an accusation of destroying evidence if a particular document cannot be located. This is commonly known as *spoliation*

of evidence and could constitute an obstruction of justice criminal offense.<sup>2</sup> The following are offered as general guidelines for record retention:

- Security incident reports: 5 years.
- Monthly or annual activity reports: 5 years.
- Annual security evaluation reports: 5 years.
- Parking violation/reminder notices: 1 year.
- Security condition reports: 6 months.
- Security officer daily activity reports: 3 months.

Security administrators should periodically review the retention periods for specific categories of records to ensure that the time periods are realistic in meeting the needs of the organization.

## References

1. On the job. (1999, March 18). *Denver Post*, p. 1C.
2. Bates, N. D. (1995). The power of paperwork. *Security Management*, 79–82.

# Patient Care Involvement

There must be a clear understanding of how the security program engages with patients and their visitors within the healthcare environment in order to properly fulfill the security and organizational mission.

The relationship or degree of security involvement with the healthcare organization's patients and visitors will vary not only according to the type of patient but also according to the location of the interaction. As an example, the security officer may have a greater need and responsibility for interaction with patients in public areas of a facility, but have rather limited contact with patients in their rooms or in clinic-type treatment areas. Likewise, security officers have a greater responsibility in dealing with visitors in parking lots and public corridors than in patient rooms.

Patients and visitors can each be viewed in two distinct groups. The patient may either be an outpatient or an inpatient. The vast majority of our discussion of healthcare security focuses on the latter. In terms of visitors, some people are visiting an inpatient, while others are accompanying a person seeking or receiving short-term medical treatment, such as in an emergency room or clinic. Types of visitors may be very diverse and include persons visiting employees; persons visiting a department for educational, information, or business purposes (salespersons, vendors, delivery persons, etc.); and persons who have no legitimate reason for being on the property (transients, loiterers, criminals, etc.).

The International Association for Healthcare Security and Safety (IAHSS) has established a Basic Industry Guideline for the role of security in patient management that should be adhered to by healthcare organizations.

**IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.04**

**Security Role in Patient Management**

**STATEMENT:** Healthcare facilities (HCFs) will develop policies and procedures that identify the responsibilities and scope of activities of security personnel in performing patient intervention activities. Patient intervention activities include performing patient watches, holds, restraints, and seclusions relative to the medical evaluation and/or treatment of patients.

**INTENT:**

- a. Management of patient care from the time of presentment of care, to the time of discharge, is the responsibility of facility clinical care staff.

- b. When security staff are involved in patient intervention activities, such intervention will be under the direction and supervision of HCF clinical care staff. Security staff may take independent action when presented with circumstances involving a clear and present danger of bodily harm or danger to property.
- c. Security officers should not be utilized as sitters or in patient watch situations for more than brief periods of time. Patients requiring one-on-one monitoring while in restraint or seclusion should be monitored by nursing assistance or other staff members with appropriate clinical training. The appropriate role for security officers should be in response to assist in patient acting out situations where the clinical staff needs help in regaining control of a patient or to provide safe transport to another location. Security officers should be utilized to supplement and not replace clinical staff members.
- d. When security staff assist in the hands-on restraint or seclusion of a patient within the facility, where physical force and/or restraint devices are required, the following will apply:
  1. There will be continuous presence, direction, monitoring, and supervision of security staff actions by qualified facility clinical care staff.
  2. Restraint devices will be those devices commonly utilized in the medical care environment that have been approved by the HCF. Handcuffs and similar law enforcement restraint devices will not be utilized unless such medical restraint devices are not immediately available and there is an immediate and clear danger that the patient may harm himself or others. It is recognized that law enforcement restraint devices may not be used in any case in specific jurisdictions. The use of weapons by security staff is considered as law enforcement use and not a healthcare intervention. The use of a weapon by security staff to protect people, or hospital property from harm would be handled as a criminal activity.
  3. Forensic patients (prisoners) presented by forensic staff should be restrained by the forensic staff supplied devices, which may include handcuffs, shackles, manacles, or like devices.
- e. Security staff will receive training as to their role with established protocols relative to patient watches, holds, and restraining patients. Training should include de-escalation and proper restraint techniques, mental health holds, Against Medical Advice (AMA) discharges as well as accreditation and regulatory agencies.
- f. Security personnel involvement in patient intervention activities should be carefully documented to include requesting caregiver, time of request, instructions given, patient name, time and duration of services rendered, and the identity of all security personnel involved in providing the support service.

**REFERENCES/GENERAL INFORMATION:**

- Stefan, S. (2006). Emergency department treatment of the psychiatric patient policy issues and legal requirements. In R. Roasch (Ed.). *American psychology – Law society series*. Oxford and New York: Oxford University Press.
- State Operations Manual, Appendix A – Survey Protocol, Regulations and Interpretive Guidelines for Hospitals, Rev. 03/17/2008. Centers for Medicare and Medicaid Services.
- Healthcare Security: *Basic Industry Guidelines*. (2007). Glendale Heights, IL: International Association for Healthcare Security and Safety.
- IAHS guideline: 02.03, Forensic Patient Security.

**Approved:** November 2007

**Last Revised:** October 2008

## Patients

The Joint Commission (TJC) has various standards that refer to patient's rights. Although for the most part these standards refer to direct patient care services, all security personnel should be cognizant of these rights as they pertain to the delivery of security services. The Johns Hopkins Hospital in Baltimore, MD, has a defined *Patient's Bill of Rights and Responsibilities* that "encourages patients to communicate openly with their healthcare team, participate in their treatment choices, and promote their own safety by being well informed and actively involved in their care."<sup>1</sup> The rights of patients are listed by every healthcare organization. Frequent patient rights the healthcare security program should be aware of and observe are listed in [Table 12-1](#).

The healthcare organization exists for the purpose of caring for the patient. Thus, all of the security program's activities must directly, or indirectly, support patient care. As such, security staff must keep the patient foremost in mind, and must always know and observe a patient's rights. Security staff must remember that the patient:

- Is the most important element in the healthcare business;
- Is not an interruption of the security officer's work but the reason for it;
- Does a favor by calling security; security does not do a favor by serving the patient;
- Is part of the healthcare business and not an outsider;
- Is not a cold statistic but a human being with feelings and emotions;
- Is not someone to argue or match wits with;
- Is a person with wants; the security officer's job is to fill those wants;
- Deserves the most courteous and attentive treatment possible;
- Makes it possible for the security officer to be paid;
- Is the life blood of every hospital.

**Table 12-1** Patient Bill of Rights

### Bill of Rights

*Patient has the right to:*

- Receive considerate, respectful and compassionate care regardless of age, gender, race, national origin, religion, sexual orientation, or disabilities.
- Receive care in a safe environment free from all forms of abuse, neglect, or harassment.
- Have pain assessed and be involved in decisions about managing pain.
- Be free from restraints and seclusion in any form that is not medically required.
- Expect full consideration of privacy and confidentiality in care discussions, examinations, and treatments.
- Access protective and advocacy services in the cases of abuse or neglect.
- Participate in decisions about your care, treatment, and services provided, including the right to refuse treatment to the extent permitted by law.
- Expect all communications and records about care are confidential, unless disclosure is allowed by law.
- See or get a copy of medical record and have the information explained.
- Receive a list of whom personal health information was disclosed to.
- Access pastoral and other spiritual services.
- Voice concerns about the care received.

*Source: Adapted in part from the Johns Hopkins Hospital, Baltimore, Maryland.<sup>1</sup>*

## Inpatients

The basic protection for inpatients comes from the nursing unit staff, which consists of nursing personnel, unit clerks, data entry persons, and ancillary staff. It is extremely rare that security personnel routinely interact with patients on a proactive security basis.

The nurse assigned to a patient is responsible for his or her total care, which includes the security and safety of the patient. Nurses do, however, receive support from the security system in protecting the patient, just as they receive support from other disciplines in administering medical care.

Nursing staff must be acutely aware of who enters the unit and for what purpose; especially during after hour periods. Just as the security role becomes more custodial during the night hours, nursing assumes a more custodial role for the patient's safety. Of course, nursing staff have a responsibility during operational periods to challenge strangers on the unit or in patient rooms at any time. In terms of strangers, it is also the responsibility of all staff to inquire of persons in their work area if they or their business is unknown. The need for this inquiry is greatest during the evening and night hours, and it increases the nearer the stranger is to patient care areas. During the late-night hours, the nursing unit often becomes very quiet, which in a sense aids unit personnel in their custodial responsibility. The quiet atmosphere means that even minor noises, such as a stairway door opening or closing, will be detected. Nursing staff must always be sharply attuned to the status of the unit.

Nursing staff should be encouraged to challenge strangers and assist them as needed. The stranger, however, becomes a suspicious person when the nurse does not feel comfortable approaching the stranger. At this point, the nurse should be encouraged to call for security support.

The nursing staff is the largest group of employees in the hospital and one with which security must continually interact. According to Kathleen Pedziwiatr, former director of nursing at Alexian Brothers Hospital in Elk Grove, IL, one of the difficulties encountered between nursing personnel and security officers is the difference in their general perception of people. On the whole, nurses are generally trusting and sympathetic, while security officers are generally suspicious. Security perceives that nurses do not always attend to security to the degree expected, due to their casual and trusting attitude. Nurses perceive that security officers often look for trouble because of their suspicious attitude. The need for both groups to communicate and understand one another is vital to good patient care and a good overall protection effort.

In addition to nurses and other unit staff, a variety of groups enter the patient unit areas to carry out their work. They include environmental service employees, volunteers, maintenance workers, physicians, therapists, technicians, and a host of other administrative and support personnel. Each of these persons also helps to protect the patient. They must investigate or report any suspicious or unusual activity that they observe. Ironically, some of these individuals have been responsible for perpetrating crimes against patients, ranging from petty theft to homicide.

## Assisting with Patients

Security officers routinely assist inpatients who are moving about the organization. More frequently, however, security is asked to assist with irrational and uncooperative patients. In some security programs this is a planned function, with security officers being an essential element of the medical care plan. In other security programs, the interaction with patients is routinely discouraged and for others, it is forbidden. The protection program that takes a “hands off” approach to patient involvement is not fulfilling an important mission for the healthcare organization. Healthcare organizations with such a security department practice should reevaluate their operating model, department role, responsibilities, and training. Historically, many outsourced security organizations have opted not to have a hands-on approach, opting instead to have an “observe and report” approach. This risk management approach is a sound business strategy for the contract agency as it can save thousands in undesired worker’s compensation expense frequently associated with uncooperative patients. Unfortunately for the healthcare organization, the risk only shifts to them and their care providers. Understanding what strategy is employed by the contract agency is an important criterion for the company selection process if an outsourced security model is employed. Sample language to call this issue to the attention of the vendor and the security selection committee is provided in Appendix II—Sample Request for Proposal for Security Service.

Responding to requests for assistance with patients is a valid and necessary function of any protection system; however, the scope of this assistance should be clearly defined. Security personnel should not take the place of medical care personnel. When emergencies occur, security officers should respond as part of the total resources available. This response is best considered a support role, and security should not assume lead responsibility for the situation or the patient unless circumstances exist involving a clear and present danger of bodily harm or significant damage to property.

The frequency of calls for assistance varies from organization to organization and depends on many factors, including the types of patients the facility serves and the availability of nursing personnel. There is a tendency for security to be called too frequently as demonstrated with a number of healthcare organizations that have witnessed their volume of security incidents for patient assistance more than double and the average amount of time spent for each event by security staff more than triple. The healthcare protection program should carefully monitor and measure their involvement in patient care for performance improvement by volume and total amount of time spent on average. Since the fourth edition of this text, the compounded effect these two issues have had on the consumption of security resources has been substantial for many healthcare security programs. Measuring and providing access to this specific data help healthcare administrators and protection professionals to better understand how the role of security staff with patient assistance can single-handedly reduce the posture of security on campus. One busy Level II trauma center in Colorado looking to improve its program after an employee survey was conducted, denoting a lack of visibility by the security staff in



the parking areas, realized that security involvement with patient assistance in the emergency room was consuming 60% of all available security resources. Another busy regional trauma center that has been tracking security involvement with patients in the emergency department has trended up from 3,000 events per year to over 4,500. In each situation, the changes to the security staffing plan were easily made as hospital administrators realized the negative effect this expectation had on their overall organization security posture.

Ironically, the better trained and more responsive the security operation, the greater the tendency to involve security officers in patient care becomes. Healthcare security administrators must review and evaluate patient-assistance activity very closely. Interestingly, behavioral HCFs generate fewer calls for assistance than do general medical facilities of the same size. This is often because employees of behavioral HCFs are programmed to care for difficult patients as a routine activity.

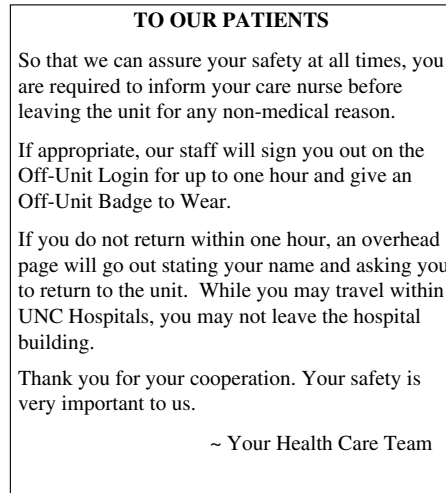
## The Missing Patient

Missing patients is one area in which patients and security staff interact. In many cases, this interaction will test the interpersonal skills of the security officer. The accountability of patients is not always as exacting as one might expect. Patients may leave the unit to take a walk, go to the cafeteria, find a place to smoke, or even visit other patients without informing unit personnel. Others may be away for tests or treatment, which may not have been properly communicated to all staff. Still others decide they do not want to remain in the facility and leave without notifying anyone of their intention. Whatever be the case, unit personnel cannot automatically sound an alarm whenever they cannot readily account for a patient. However, when a patient is clearly missing, or there are extenuating circumstances, the unit staff should notify security. Extenuating circumstances may involve the mental state of the patient or situations in which the safety of the patient may be in question. To prevent unnecessary searches, many units have procedures in place for patients to sign out or otherwise communicate with the nursing staff before leaving the area. [Figure 12-1](#) is a notice which The University of North Carolina Hospital posts throughout their facility to keep patients from leaving the hospital without communicating to medical staff.

The two most important factors relative to security involvement in the missing patient incident are timeliness and thoroughness of the search. The probability of a successful search decreases as time increases.

Specific guidelines should cover the actions and responsibilities of the security officers in investigating missing patients. Officers should thoroughly search the common and support areas of the facility, including food service areas, corridors, lobbies, lounges, public washrooms, parking areas, and the grounds. Unit personnel and other staff should search other patient and treatment areas.

When missing patients are located, officers should attempt to convince the patient to return to the unit voluntarily. The hospital bears responsibility for patients who may be



**FIGURE 12-1** Notice to patients (Courtesy of the University of North Carolina Hospitals, Chapel Hill, NC).

irrational. Security officers should use extreme caution in chasing or yelling at patients, because an irrational patient can easily be panicked and might fall or run into a street. Officers should also try to summon medical personnel to assist in returning the patient to the unit. Officers should not use physical force unless they are so directed by a competent authority or, in their judgment; the patient is clearly endangering his or her life or the lives of others. This is a delicate judgment. Officers can be held liable for false arrest or assault and battery if they detain patients against their will. In all instances, officers must complete a detailed incident report describing all the facts of the situation and the action taken.

As a general rule, security should begin their search on the boundary of the campus and work inwardly, while other hospital staff begins searching on the unit floor and expands outwardly. It is important also to address questions as to how far off the property the search should be conducted and at what point law enforcement should be notified. Property lines should not be used as a “line in the sand” in terms of searching. The search should include blocks surrounding the property; however, this off-property search is generally conducted as a secondary phase to the initial search. A missing patient incident that took place in Pennsylvania illustrates this point. An intensive care patient left his bed at approximately 3:00 A.M. The responsible caregiver notified security within minutes of the situation as she heard the monitoring alarm sound while she was caring for another patient. Security searched the facility and grounds to no avail. At approximately 6:00 A.M., the police were notified by passers-by of a man in a hospital gown lying in the middle of the sidewalk approximately one block from the hospital. The patient, with Foley catheter still in place, was dead.

For patients who have left the facility without informing staff, the response to their absence is based on what is reasonable for the particular situation. For some organizations, an absence of 45 minutes triggers the missing patient protocol and patient search. It should be noted that the length of time for initiating action will vary by the time of day. A patient missing for 45 minutes in the middle of the afternoon is quite different from a patient missing for even 15 minutes at 3 A.M. Other organizations deem elopement response necessary when it becomes reasonably certain the patient is missing without authorization. All HCFs should have the capability to conduct an appropriate search of the premises within 30 minutes of a missing persons report. At the time the initial search is completed, and certainly within 45 minutes of a negative search, the police should be notified. Special situations may reduce this time frame appropriate to the information available.

If the search is unsuccessful, officers should report back to the patient care unit to detail their actions and state the outcome of the search. In some cases this report will be directed to an incident command center if the organization has activated such a center in response to the missing patient incident. It is not within the general scope of the security program to assume responsibility for anything more than the search. Notifying the administration, the physician, or the family should not fall within the responsibility of the protection officer. See [Figure 12-2](#) for a sample missing patient search form.

A common medical record form used in many hospitals is the AMA form. It is normally used for patients who, after admission, decide they do not want to stay in the hospital. If unit personnel cannot persuade these patients that it is in their best interest to remain, the patients are asked to sign the form stating that they acknowledge that they are leaving AMA. Patients can refuse to sign the form and should be allowed to leave.

Leaving AMA is different from patient elopement or patient wandering and is determined by the patient's decision to leave the facility having been informed of and appreciating the risks of leaving without completing treatment.<sup>2</sup> Most adult patients are legally able to discharge themselves without completing treatment.

Sometimes when security officers are advised of a missing patient, they discover the patient leaving the facility and getting into a cab or parked vehicle. Officers should, of course, try to persuade the patient to return to the unit. Reluctant patients can often be convinced to go back to the unit, supposedly to sign out. This gives unit personnel a chance to talk further with them. Once back on the unit, patients may be more easily persuaded to remain, or to at least to wait until their doctor can be contacted. The University of Pittsburg Medical Center, in response to the death of an 89-year-old patient who had dementia, introduced new search procedure for missing patients called "Condition L." Initiated by the nurse on the unit and announced overhead throughout the hospital, the code "summons every available employee including those in security, nursing, maintenance, and environmental services to assist in a coordinated search of the hospital complex."<sup>3</sup>

The issue of missing patients is not isolated to acute care hospitals in the United States. Farnham Road Hospital, a psychiatric hospital in Surrey (UK), reports missing

### Missing Patient Search Checklist

Patient Name:	Unit:	Room Number:
Date of Elopement:	Search Coordinator:	
Search Start Time:	Search End Time/Date:	
<b>AREAS SEARCHED (To be completed by all units participating in search):</b>		
_____ Patient Rooms _____ Public Bathrooms _____ Linen rooms _____ Janitorial Area _____ Soiled Utility Areas		_____ Kitchen Area _____ Stairwells _____ Locked Areas _____ Waiting Areas _____ Other:
Unit Searched:	Search Start Time:	End Time:
Responsible Director/Supervisor:		
Names of Who Was Involved in Search		
<b>PLEASE CALL SEARCH COORDINATOR WITH YOUR RESULTS. FORWARD THIS FORM TO RISK MGMT</b>		

\_\_\_\_\_  
Signature of Search Coordinator

\_\_\_\_\_  
Date Forwarded to Risk Management

**CONFIDENTIAL**

**FIGURE 12-2** Sample missing patient search form.

patients to the police at a rate of two a month. In May 2007, the hospital reported seven patients missing for a total of 77 days before being recovered safely by the police.<sup>4</sup>

### Patient Elopement Prevention and Response

Finding that a patient has “gone missing” is a scary situation for providers and patients’ families. According to the Veterans Administration (VA) National Center for Patient Safety, elopement is defined as: “A patient that is aware that he/she is not permitted to leave,

but does so with intent.”<sup>5</sup> In many cases of elopement, the patient may have a decreased mental capacity related to a number of medical conditions to include dementia or altered mental status or acute alcohol intoxication. Despite the level of capacity or intent, eloping patients are often at risk for serious harm, and there are many cases where patient elopement has resulted in serious injury and death.

TJC’s sentinel event policy defines “any elopement, that is unauthorized departure, of a patient from an around-the-clock care setting, resulting in a temporally related death (suicide, accidental death, or homicide) or major permanent loss of function” as a reportable sentinel event.<sup>6</sup> This reporting requirement reflects the level of harm to the patient regardless of the patient’s intent to leave or mental capacity. According to TJC sentinel event statistics, the primary contributors to elopement are breakdowns in patient assessment and team communication.<sup>7</sup> Protection of patients from elopement risks requires attention to preventive measures through assessment and elopement precautions as well as appropriate intervention after elopement occurs.

Adequately assessing patients for elopement risk factors and use of elopement precautions can, in many cases, prevent elopement and improve safety. Such an assessment and possible precautions have been outlined in an elopement tool kit created by the VA National Center for Patient Safety. A “yes” to any of the following assessment questions often indicates that the patient is at risk for elopement:

- Does this patient have a court-appointed legal guardian?
- Is this patient considered to be a danger to self or others?
- Has this patient been legally committed?
- Does this patient lack the cognitive ability to make relevant decisions?
- Does this patient have a history of escape or elopement?
- Does this patient have physical or mental impairments that increase their risk of harm to self or others?<sup>8</sup>

The security officer is often asked to watch or stand by for the patient meeting any of the above criteria. When a security officer is on a “watch,” the primary objective is to keep the patient safe and prevent patients from harming themselves or others.

Every healthcare organization should have a defined patient elopement response procedure that is initiated when any patient is believed to have left the facility without authorization. Many organizations will have a “code” to initiate an organizational response. If an elopement occurs, it requires both actions by the care providing staff in the area from which the patient is missing as well as an organization-wide search usually led and coordinated by the security staff. A typical protocol includes the following steps:

- Notification of the operator by unit staff indicating a code/elopement;
- Notification of security with a description of the missing patient and pertinent clinical information;

- Notification of the patient's physician;
- Immediate search of the unit and surrounding area by unit staff;
- Immediate search of hospital and grounds by security personnel;
- Notification of the patient's family by the physician;
- Notification of police by security as appropriate;
- Notification of appropriate administrative personnel.<sup>9</sup>

Procedures differ among organizations. However, the key is to do what is reasonably necessary to return the patient to a safe environment. In some instances the patient may not be located and law enforcement must be called to solicit their response in the search for the patient. The agency should be supplied with the following data concerning the patient:

- Name;
- Physical description: age, height, color of hair, weight, identifying marks (scars, tattoos, etc.), and what the patient was wearing;
- Mental status: confused, suicidal, on a psychiatric or alcohol hold;
- Risk status: does patient have an IV line; medical condition that is being monitored or needs monitoring.

The healthcare organization should have policies and procedures in place indicating the steps that personnel are to follow in any elopement situation, and adequate training should be provided for all staff. These protocols should include prevention procedures needed to reduce the risk of an elopement. A simple but very effective risk reduction measure is to require the patient to wear a hospital gown or pajamas at all times. Removing all personal clothes and belongings is a psychological deterrent to leaving the facility and helps readily identify the patient if a search ensues.

Other preventative measures may include placing the patient under constant observation or locate the patient close the nursing station, placing an electronic monitoring device on the patients (if available). Some healthcare organizations use "specialized sitters" to sit with patients who are at risk for elopement. Based on the medical unit and need, security design considerations can be used to prevent elopements. Time-delayed locks, closed-circuit television (CCTV) cameras with audio capability, and radiofrequency (RF) devices have all been used to help successfully prevent patients from eloping.

A patient elopement is a reportable event to a number of external regulatory agencies. The healthcare organization should denote specific responsibility for who should fulfill this requirement. Often, this is the responsibility of the risk management function. Rarely, does the initial report involve the healthcare security administrator. However, follow-up investigative activities by the various regulatory agencies do frequently involve the protection program.

The IAHS has created a Basic Industry Guideline for the prevention of and response to patient elopements that every healthcare organization should adhere to.

**IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #09.04****Patient Elopement**

**STATEMENT:** Healthcare facilities (HCFs) providing inpatient services will develop a multidisciplinary procedure for preventing and responding to patient elopements. The procedure should distinguish between elopements; wandering; and leaving “against medical advice” [AMA].

**INTENT:**

- a. Definitions:
  1. Elopement is generally defined as a patient incapable of adequately protecting himself or herself, and who departs the HCF without the knowledge and agreement of the clinical staff.
  2. Wandering refers to a patient who “strays” beyond the view or control of clinical staff, causing concern, but without the intent of leaving.
  3. Leaving AMA is determined by the patient’s decision to leave the facility after being informed of and understanding the risks of leaving without completing treatment.
- b. Elopement prevention procedures are generally a clinical responsibility, and should include:
  1. Assessing each patient’s elopement risk during the admission process and reassessing such risk, as indicated, during the patient’s stay.
  2. For patients at a high risk of elopement, steps should be taken to minimize the likelihood of a successful elopement such as:
    - Assigning such patients to rooms nearer and more visible to clinical staff;
    - Some HCFs now dress patients identified as being at significant risk of elopement in uniquely colored gowns, which can be easily identified by others in the HCF;
    - Additional measures may include assignment of a sitter or use of Radio Frequency Identification (RFID) to track patient location.
  3. A means of identifying patients that are authorized to leave the unit. Some facilities develop log on and off unit pass systems to prevent unnecessary facility searches and to identify patients away from their units without approval.
- c. Elopement Response Plans should address the following:
  1. Clinical staff on duty at the time of a wandering or elopement event will conduct a search of the floor and adjacent areas as indicated and notify the security department if the patient is not found.
  2. The security supervisor on duty or security designate, as identified in IAHSS Healthcare Security: Basic Industry Guidelines 02.01, will organize a search of the facility’s buildings and grounds. Consideration should be given to assignment of staff working near facility exits. Some HCF enlist help via an overhead page using a unique code—combined with an e-mail or other mass notification alert.
  3. If the patient is located on the grounds, security should notify clinical staff and attempt to return the patient to their unit.

4. If the patient is not located within a reasonable time, law enforcement should be notified to obtain assistance in initiating a wider search.
5. An HCF employee should be identified to coordinate information sharing and other follow-up with law enforcement.
6. An HCF employee should be identified to coordinate notification of and coordination with the patient's family.
7. If the patient returns to the HCF, security should meet with clinical staff to evaluate the status of the patient, and possibly develop a plan to prevent the patient from engaging in another elopement.
8. In the event of a reported patient wandering or elopement, an Incident Report should be written in accordance with 05.01 of IAHSS Healthcare Security: Basic Industry Guidelines.

#### REFERENCES/GENERAL INFORMATION

- Gerardi, D. (December, 2007). Elopement. <http://www.webmm.ahrq.gov/case.aspx?caseID=164#ref5> (Accessed February 11, 2008).

**Approved:** April 2008

## The Security Watch

Providing an appropriate safe treatment environment for all patients is a basic requirement of every healthcare organization. Clinical staff are expected to implement appropriate interventions, as needed, to prevent patients from harming themselves or others. Often this will include security officer support to provide constant monitoring to help protect the patients from harming themselves, harming a care provider or others, or to prevent the patients from leaving the facility. This security support activity is commonly referred to as a “Security Watch.”

In most healthcare organizations the nurse assigned to the patient is responsible for determining the need for the security watch and notifying the physician when a patient is placed on a security watch. Generally, most nurses do not receive specific training or guidance on how to evaluate patient behaviors from the perspective of the security risk posed. The result is inappropriate use of the security officer for patient intervention. A system of seven Denver-based hospitals realized the absence of training and specific guidance to their care providers was driving their security costs beyond their budgetary control. The system of hospitals collectively addressed this issue with the development of “At-Risk” patient criteria to guide their nursing staff and physicians. The system defined patients to be at risk if they have or are:

- Been placed on a mental health or alcohol hold in accordance with state law;
- Acute drug/ETOH intoxication;
- Head-injured with altered mental status;
- Confused to time, place, and/or person;



- At risk for elopement based on past history or current condition;
- Disruptive or violent (patient may lose control, threaten to lose control, or give others evidence of a deteriorating mental condition);
- Indication(s) of a weapon or other dangerous item.

An important element for every healthcare professional to understand is that any patient on a security watch is the direct responsibility of the nurse assigned to that specific patient. The nurse directs all action regarding the patient and cannot relinquish this responsibility to the security officer. The officer's involvement in this patient care procedure is merely an extension of the assigned nurse; all actions taken with the patient is on behalf of the care provider. Creating guidelines to govern the relationship of the officer with the assigned nurse and the patient with specific responsibilities outlined for the security officer is a must for every healthcare protection program.

The security officer should never give the patient anything without the nurse's permissions. The officer should remain alert for signs of increased patient discomfort, distress, or aggressive behavior and be instructed to notify the assigned nurse immediately. In the event of an emergency involving a patient, the security officer should assist as directed by the healthcare staff. In the event the emergency endangers the patient and there is no time to consult the healthcare staff, the security officer should take action to control the immediate threat and seek healthcare staff direction as soon as it is available.

The assigned nurse should continually assess the patient's ongoing need for a security watch, at minimum, every hour. In the event multiple security watches are required by a single officer, patients should be consolidated into close proximity (e.g., adjacent/ adjoining rooms). Together, unit staff and security personnel should evaluate the need for additional security personnel anytime a single security officer is asked to conduct more than one security watch at a time.

The security officer should be well integrated in the healthcare delivery team. When assigned to watch a patient, officers should be required to stay at the door of the room or as close as possible without causing an adverse effect on the patient or the care of the patient. The officer should be careful not to allow the security uniform to excite or antagonize the patient. Keeping the patient in a line-of-sight should be a fundamental responsibility. In watching multiple patients, it is important for the officer to move continuously from room to room and maintain frequent and periodic sight of each patient.

Documenting all involvement with the patient on a security watch is an essential component of the security officer's role and function. Using the Security Incident Report or other data capturing tool defined by the healthcare organization, information collected should include:

- Name of the assigned nurse initiating the security watch;
- Time the watch begins;
- Patient name and number;
- Name(s) of other medical staff member(s) giving direction to the officer during the watch;

- Physical contact with the patient including aggressive behavior by the patient;
- Type of restraints applied or removed (including which limbs were involved) with the officer's assistance;
- Name of the medical staff members involved in the application and/or removal of restraints;
- Name of each officer providing relief or assistance during the watch;
- Beginning and ending times of relief or assistance;
- Name of the assigned nurse ending the watch;
- Time the watch ends;
- Temporary or permanent relief officers should continue the initial Security Incident Report by noting the change of officer in the body of the text.

In all instances in which security has assisted with patient restraint, officers should complete a report detailing this assistance. [Figure 12-3](#) shows a sample of a patient restraint form. Depending on the degree of interaction involved, a Security Incident Report may also be required.

Most healthcare professionals agree that mental health patients are a significant factor in the explosive increase in the volume of security watches in the emergency department and elsewhere in the HCF. Many hospital emergency departments specifically have responded by taking a page from the standard security practices employed in behavioral health care facilities for many years. This includes:

- Requiring armed security officer to secure their sidearm in a proper storage unit, before conducting a security watch;
- Removing all sharp objects from the room with meals served on disposable trays with plastic spoons and paper plates/cups;
- Requiring all at-risk patients on a security watch to wear a hospital gown or pajamas;
- Removing all personal clothes and belongings from the at-risk patient's room (secured per the hospital patient valuables policies).

If an at-risk patient refuses to release his/her clothing or belongings, a search should be conducted to verify that the patient does not have possession of dangerous items or other hazardous paraphernalia that could be used to harm himself/herself or others. The healthcare organization that employs the practice of searching patients should provide specific guidance to the security officers.

### *Patient Search*

If a patient search is required, the security officer should always attempt to obtain verbal consent from the patient before conducting the search. If consent is not received, many security officers have often found success asking the patient a second time to release his/her clothing and belongings. If the patient does not comply with either request, unit staff and security personnel should confer with the physician and possibly

<b>PATIENT NAME AND ID#:</b>			<b>UNIT:</b>				<b>ROOM NUMBER:</b>		
<b>RESTRAINT START TIME/DATE:</b>			<b>RESTRAINT END TIME/DATE:</b>				<b>TYPE OF RESTRAINT:</b>		
Time	Visual Alert/ Sleeping, Belligerent, Confused	Pt Obsv 30 Mins	NV 2 Hrs	Fluids 2 Hrs	Elim 2 Hrs	Vital Signs 4 Hrs	Food 6 Hrs	Comments	Initials

**OTHER COMMENTS** \_\_\_\_\_

\_\_\_\_\_

Initiating Care Provider:	
Ending Care Provider:	
Total Time Spent by Security:	

\_\_\_\_\_ (Initials)

**FIGURE 12-3** Sample security patient restraint form.

risk management or other appropriate personnel to include family members to determine the best course of action to include the risk and benefits of searching the patient. There may also be a need to seek police or other assistance. In a growing number of healthcare organizations, where there appears to be no reasonable solution to consent for the search or release of clothing and belongings, the hospital and physician have elected to discharge the patient in response to the security risks presented by the patient. A discharge decision is never made by the healthcare security staff and at best is a decision of last resort.

In 2009, Beth Israel Deaconess Medical Center adopted a policy that permits patients to remain in their own clothes unless they pose an imminent risk of injuring themselves or others. In those circumstances, forcible removal is permitted only after other less intrusive methods to ensure safety have been unsuccessful and federal standards that limit the use of physical restraint are met. In the same year, the Massachusetts Departments of Public Health and Mental Health jointly drafted a statement declaring that psychiatric patients have a right to retain their clothing and that forced removal is a form of physical restraint that cannot occur unless compelling clinical information indicating imminent risk to self or others exists.<sup>10</sup>

When consent for the patient search is received, it should always be conducted by a person of the same gender as the patient, in an area affording patient privacy, and in the presence of a physician or an assigned caregiver; never alone.

A search procedure must be developed and training provided relative to a methodical approach for how to conduct the search. The “airport screening method” is frequently used as outlined in the patient procedures in [Figure 12-4](#).

The IAHSS has a Basic Industry Guideline for searching patients and patient areas for contraband that should be followed for healthcare organization to reduce the likelihood of contraband entering the facility.

#### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.08

##### **Searching Patients and Patient Areas for Contraband**

**STATEMENT:** Healthcare facilities (HCFs) should establish procedures to reduce the likelihood of contraband entering the healthcare setting. Searches of patients, patient belongings, and patient areas should be conducted as needed.

##### **INTENT:**

- a. These searches are undertaken to reduce the likelihood of potentially dangerous, illegal, or other items which may be contrary to the patient’s treatment plan from being brought into the HCF.
- b. Contraband includes, without limitations, any type of weapon, illegal or unauthorized drugs, intoxicants, flammable items, and sharp-edged objects. Other items may be prohibited, based on patient needs as determined by medical staff.

- c. A room search and a personal search protocol which respect the dignity of the patient should be established. The protocol should include:
  1. When a search is justified;
  2. Who may initiate a search [usually medical or nursing staff];
  3. Who conducts the search [usually security along with a unit caregiver];
  4. How a search should be conducted, both of a person and an area;
  5. How search results are to be documented;
  6. How seized items are to be handled, safeguarded, and ultimately disposed of, allowing for, as appropriate (a) destroying and discarding; (b) turning over to law enforcement; or (c) returning the item(s) to the owner or a responsible family member.
- d. These searches and inspections are administrative in nature, and are not law enforcement searches. It is not the intent of this guideline to provide law enforcement with evidence to criminally prosecute or otherwise act on the basis of items seized during such inspections. Nor is it the intent of this guideline to prohibit the turning over of such contraband to the appropriate law enforcement jurisdiction. The HCF's search protocol should address who may, and under what circumstances a determination will be made to involve a law enforcement agency.

**Approved:** April 2009

## Patient Risk Groups

Certain patient risk groups require specific attention relative to security. These basic groups are identified by patient type and include the VIP patient, the infectious patient, the combative patient, behavioral health patients, patients with autism, the forensic patient, the wandering patient, and the infant/pediatric patient.

### The VIP Patient

The VIP patient is any patient who poses special security problems and may require certain security precautions to be taken. For celebrities and high profile politicians, strict visitor control procedures may be required. In some cases these patients are accompanied by their own security personnel. The hospital's protection service thus has little responsibility for the patient's security. This is especially true when a government figure is involved. Special telephones, quarters for protection personnel, special visitor passes, and the like may require consideration.

The second major type of VIP patient requiring security safeguards for the patient who has been threatened or beaten, is a victim of a crime or a witness, or is involved in an activity that puts him/her a risk of being harmed during treatment. Once the treating organization is aware of such potential danger, there is a responsibility on the part of the

1. Ask the patient to face the searcher with arms outstretched and feet slightly spread (airport screening method). The searcher will start at the top of the head and continue in a clockwise direction until the patient's body has been outlined, the extremities searched, and the torso patted down from shoulders to lower hips both front and back.
2. Whenever possible, the searcher should use the back of a hand to conduct the search. If the patient has short hair only visual inspection is required; however, long hair or up-swept hairdos must be patted down. Remove and search all head coverings (turbans, bandannas, hats, etc.).
3. Search the patient's arms by encircling the arm with the hands and moving downward from the shoulder to the bottom of the sleeve in one motion.
4. Search the patient's legs starting at the back of the leg (using the back of the hand) moving downward in an overlapping paths, until the patient's entire lower body has been searched. In most cases, do not search the patient's shoes unless there is reason to believe the patient is attempting to conceal something.
5. After the patient's body and extremities have been completely outlined, raise the patient's arms and search the torso starting at the top of the shoulders (again using the back of hand) moving downward towards the hips. Overlap each pass until the patient's entire torso is searched. Repeat the same procedure for the patient's back. Give special attention to the area of the back near the waist caused by the curvature of the spine and under the armpits.

NOTE: Generally, a search should encompass no more than a pat down of the individual's outer clothing; however, it should be done with sufficient care and strength to feel a concealed weapon.

6. If, during the course of a search, suspect items are found, ask the patient to slowly remove the item from its location. Obtain the item from the patient. Circumstances may require reaching into a pocket or other hidden areas (i.e., a boot) to retrieve a suspected hidden weapon. Exercise caution about where hands are placed—LOOK BEFORE YOU TOUCH ... TOUCH WHERE YOU ARE LOOKING.
7. Perform all bag and belongings searches in a systematic, circular, and clockwise path. Start the search with a visual inspection of the exterior. Search the interior of the bag in the same circular motion—feeling the top, sides, and bottom of the inside of the bag.
8. Restrict the patient's access to the contents of the bag and keep the bag out of public view. Do not allow the patient to place his/her hands into the bag until the search is complete.
9. Remove all items from the patient's room. Return all items upon discharge. Place all removed personal items in a valuables envelope and process through the patient valuables system. Place all other patient items in a plastic bag for safekeeping until the patient is transferred or discharged. Inventory and label the bag with the patient's information.
10. Turn over to the Pharmacy all medications and unidentifiable substances for identification anonymously. Pharmacy will properly dispose of all illegal substances or turn over to the police anonymously.
11. Secure all weapons and turn over to the patient's representative or police department if appropriate.
12. Searches should be documented, including the patient's consent to search, the time and date of the search, the personnel conducting the search, patients or family members present, reasons for search, and whether any contraband, weapons, or dangerous objects were found and disposition of such items.

**FIGURE 12-4** Patient search procedures.

organization to take preventive steps. These steps will vary according to the degree of risk and include:

- Controlling information about the patient to include removing the patient's name from the general patient population database. That way, if someone inquires about the patient at the telephone information center or information desk, the operator will indicate that there is no such patient.
- Disconnecting all telephone service to the patient's room.
- Moving the patient to a room that provides maximum surveillance by unit care staff.
- Restricting or denying visitors.
- Providing a patient companion, or sitter, to be with the patient at all times.
- Providing a security guarding arrangement. This would involve the patient who would not be under police control or custody. (The handling of the forensic patient is considered to be in a different patient risk group.)

Figure 12-5 shows an example of a security VIP policy.

Dale Schoolfield, CHPA, Security Manager for Provena Saint Joseph Hospital in Elgin, IL, wrote in his evaluation of the hospital's very important person policy to include victims of violence. He described the need to have a policy in advance of a gang victim arriving at the emergency department to avoid situations where staff and visitors are put into danger. Highlights of how he helped his hospital amend its VIP policy included:

- Immediately registering patients of the Emergency Department as a result of a violent act as no-published patients with no information given to anyone except law enforcement.
- Limiting visitation to immediate family only and no more than two visitors.
- Notifying administrative coordinators, telecommunications staff, marketing/public relations, and the administrator on duty of the situation and that NO patient information is to be given to the news media or anyone walking in or calling the hospital.
- Ongoing evaluation of the need to restrict access into the emergency department and/or hospital.
- Counseling family members regarding the safety procedures and the need for privacy and confidentiality of the patient.
- Ongoing evaluation of the potential for a breach of patient security due to excessive visitors arriving at the hospital with patient information.
- Increasing security officer patrols in the area.
- Critiquing the incident and organizational response afterward to identify opportunities for improvement.<sup>11</sup>

## The Infectious Patient

When assisting with patients, security personnel have long been concerned about inadvertently contracting an infectious disease. This concern has been heightened by the

**Example**

**HEALTHCARE SECURITY  
POLICY AND PROCEDURE  
FOR  
THE VIP PATIENT**

**GENERAL**

The VIP patient is any patient who requires special protection measures during outpatient or inpatient medical services. This patient may be a high profile public figure, a celebrity, or a patient whose circumstances or information indicates that he/she may be in some elevated degree of danger.

**PUBLIC FIGURE/CELEBRITY**

Except for emergency treatment or admission the protection of this type of patient is generally preplanned. In many cases the security department will coordinate protection safeguards with the VIP's personal security staff or a public safety agency such as the police, secret service, or FBI.

**PATIENT IN DANGER**

This patient may be in danger due to threats to the family or directly to the patient, the result of a gunshot wound, stabbing, gang or criminal activity, or being a witness to a major crime.

**PROCEDURES**

The same type of security safeguards and procedures will be utilized for each type of VIP. However the degree of the security precautions and activity will vary with the specific patient situation. In general the security precautions and safeguards could include the following actions:

1. Notify appropriate organization personnel including Risk Management, of patient identity and circumstances requiring increased VIP security measures.
2. Notify public safety agencies if deemed appropriate and/or co-ordinate efforts with these agencies.
3. Assign a patient room that is away from elevators and fire stairwells or exits.
4. If security officers, bodyguards, or forensic staff will be utilized assign a patient room at the far end of a dead-end corridor. If this type of personnel is not utilized assign the patient a room close to the nursing station where good surveillance of the room can be maintained.
5. Remove the patient name from the patient information system, Front Desk, and census reports, substituting an assumed name for the actual patient.
6. Maintain the patient's chart in the patient's room.
7. Brief the nursing unit staff of general information and/or specific action items required of medical care staff.
8. Determine if any visitors will be allowed.
9. Obtain name and telephone number of person(s) co-ordinating security for the VIP who can be contacted as questions arise or if there is an emergency. This contact person may be a family member.
10. Utilize security officer briefing procedures to communicate information to all security personnel.

**FIGURE 12-5** Sample VIP policy and procedure.

advent of AIDS and the increase in hepatitis-B infections. AIDS patients are in the final stages of a series of health problems caused by a human immunodeficiency virus (HIV), which can be passed from one person to another through unprotected sexual contact with an infected partner, the sharing of intravenous drug needles and syringes, the



exchange of body fluids, and, less frequently, blood transfusions. There is no known risk of infection in most of the situations encountered in daily life and no evidence of transmission of the AIDS virus by everyday contact.

By the nature of their occupation, healthcare workers, including security officers, are likely to come in contact with people infected with AIDS or hepatitis B. The major occupational risk for healthcare workers is the contact of their skin or mucous membranes with infected body fluids or tissues. Exposure can occur from needle stick, cut injuries, and splashes of blood. The virus has also been linked to other body fluids, including semen, preseminal fluid, vaginal secretions, and human breast milk.

For security personnel, the risk of exposure to AIDS or hepatitis B in the course of normal duties is extremely low; exposure could occur only under unusual circumstances. It is possible that security officers might sustain cuts or puncture wounds or be stuck by a needle while assisting with or searching patients or dealing with suspicious people. The risk of infection from being bitten by an infected individual is considered to be low.

The first step security management should take is to fight fear with facts. Employees should be reassured that there is little reason to fear that they will be exposed to infection. Continually educating security staff about the nature of AIDS and how it can be transmitted and informing them of the availability of any emergency equipment will do much to alleviate fear.

Legal issues should not be overlooked when educating personnel about AIDS. A suit was filed against Kings County Hospital in Brooklyn, NY, by a doctor who contracted the AIDS virus when she was stuck by a needle left among gauze on a patient's bed. The suit claims negligence and breach of contract because a safe workplace and safety equipment should have been provided and the defendants should have warned and trained staff members about the dangers of AIDS-infected needles.

Another legal element that must be considered is invasion of privacy. If a staff member released information about an AIDS patient and that patient lost his or her job, the value of the lost income would most likely be sought in a lawsuit. Security supervisors can protect such information by:

- Reporting known infractions of organizational policies regarding patient information;
- Reminding security officers to keep all security reports and other organizational documents confidential;
- Taking appropriate steps to discourage talk among employees about any patient.

## The Combative Patient

Security personnel assist with combative patients most often in four areas of the facility: the emergency department, the intensive care units (ICUs), the mental health areas, and the general nursing unit and medical clinics. To provide patient assistance regarding

combative patients, all security personnel should be well trained in verbal and nonverbal de-escalation measures and restraint procedures.

### *Emergency Department*

The emergency department requires frequent security assistance, especially in facilities that treat many drug overdose patients, patients with injuries due to shooting or stabbing incidents, and patients with mental health or alcohol/drug impairments. This section of the text primarily concerns the security officer's interactions with patients and staff in the emergency department.

Other security concerns for this department are discussed in *Chapter 19, Preventing and Managing Healthcare Conflict and Violence*, and *Chapter 20, Security Sensitive Areas*. Belligerent and intoxicated patients may also require security assistance, particularly when they are brought for medical care against their will. These patients are often brought to the medical care treatment facility by law enforcement authorities, ambulance crews, or friends/relatives; often the transporters are more aware of the treatment needed than the patient is.

When friends or relatives are present, there is an added concern for the protection officer. If the accompanying persons are intoxicated or drug impaired, they will require control or at least surveillance. They can easily become annoyed or angered at delays in treatment, or they may have their own ideas of what treatment is required. Emergency physicians have estimated that more than 75% of patients and visitors to some inner-city emergency departments are under the influence of drugs.

Emergency department clerks and triage nurses are generally the first staff members to interact with persons entering the department. They must be stationed to observe persons entering the department, to provide service and directions, and to keep the area under surveillance to detect persons in distress.

A growing trend in larger security operations, and in areas with an established history of frequent harmful situations, is to station a security officer in the emergency department 24 hours a day. A response some hospital emergency departments have taken after very serious security incidents that resulted in significant staff injury or death is the deployment of off-duty police officers in the waiting area. The emergency room staff must be alert for impending disruptions. When they suspect trouble, they should call for a security presence. The only preventive action required may be for a security officer to patrol through the area or to stand by unobtrusively.

In smaller security operations, a security officer may be assigned to the emergency room during peak periods. In one small hospital, an officer is assigned every Friday and Saturday night between 7:00 P.M. and 3:00 A.M.

The American College of Emergency Physicians (ACEP) believes that optimal patient care can be achieved only when patients, healthcare workers, and all other persons in the emergency department are reasonably protected against violent acts occurring within the department.

To ensure the security of the emergency department environment, the ACEP states that the hospital has the following responsibilities:<sup>12</sup>

- Provide a best practices security system including adequate security personnel, physical barriers, surveillance equipment, and other security components.
- Coordinate the security system with local law enforcement agencies.
- Develop written emergency department protocols for violent situations occurring in the emergency department.
- Educate staff on preventing, recognizing, and dealing with potentially violent situations.
- Conduct ongoing assessments of emergency department security system performance.

Overcrowded emergency departments contribute to patient distress and increase the likelihood of adverse outcomes—elopement, self-harm, and violence. Many organizations have introduced initiatives to improve waiting times to decrease incidents of violence to include fast-tracking initiatives for patients with behavioral health problems.

### *Intensive Care Unit*

Many healthcare organizations have realized that after the VIP or combative patient is discharged from the emergency department, he/she is not always ready to go home. The most chronic problems are channeled to the ICU or other critical care units. The frequency of security officer involvement with patients on these units requires the protection program to prepare for how it will respond to calls for service. Many healthcare organizations have begun to deploy consistent systems and process in these departments as those utilized in the emergency department. Specifically, the capability to control and restrict access when at-risk patients are present is a needed precaution. The restricted access control system may not be operational at all times; however, the ICU must be able to convert to this higher level of security quickly—ideally with the push of a button.

The waiting areas of the ICU are a common location for family members and visitors of the patient to express great emotion and expose the protection program to many cultural customs. Tension is commonly found in the waiting area, and security officers often respond due to loud grieving by family members, the need to de-escalate feuding siblings who hold different opinions about end-of-life decisions, or manage an extremely large influx of visitors that may accompany a patient.

The ICU waiting area is often reflective of the many customs and cultures prevalent in every community. The security officer must be culture-sensitive. An important attribute of the security officer is to be sensitive to different customs and understand that different cultures often behave differently. This may include the process of grieving, different level of involvement with a patient, nontraditional religious or family rituals, as well how they may react to authority figures. For example, security officers responding to a disturbance call in the ICU waiting area may arrive and find that a large family has just found out that their loved one has passed away. The grieving process may be loud and a

difficult experience for other visitors. However, the culturally sensitive security officer will quickly realize that the disturbance call is not a security issue at all and work to identify a location for the grieving to occur without disrupting others.

### *General Nursing Unit*

Another category of patients who require assistance is the traditional patient on the nursing unit. In some cases, patients not previously diagnosed as possible combative patients may suddenly and unexpectedly develop irrational behavior. Generally, the nursing staff is not prepared to handle this unpredicted behavior and must seek off-unit resources.

Regardless of the situation, security officers should not be forced to render medical judgments. They should base their actions on specific instructions from a nurse or a physician at the scene. If these instructions are not forthcoming upon their arrival, officers should determine who is in charge and inquire about his/her role and necessary actions. At all times, security officers should act to assist and support rather than assume primary responsibility. The more responsive security is in providing patient assistance, the more often they will be called.

### *Medical/Dental Clinics*

General medical/dental clinics can be an area of disturbances caused by both patients and visitors. There are at least two factors creating conditions for such problems: the large number of people who frequent these facilities and the length of time patients must wait to be served. It is not unusual for a clinic patient to have four or five persons accompanying him/her. These “visitors” are often infants and small children, which can add to confusion and frustration. Extended clinic hours have reduced instances of disruptive behavior, as parents are less likely to bring their children, as sitters become more available in the evening hours.

## **Behavioral Health Patients**

Numerous studies have cataloged the substantial problems facing behavioral health patients and healthcare organizations and their protection efforts. Behavioral health disorders are a major concern for healthcare organizations everywhere. Every hospital treats patients with behavioral health disorders even when an acute care hospital has no organized behavioral health service or psychiatric clinical specialists.<sup>13</sup>

A national and international dilemma has been created with the diminished capability of behavioral health services in most communities. When coupled with the significant underfunding of public agencies historically responsible for behavioral healthcare, a shifting of costs and care for these patients has moved to the general hospital.<sup>14</sup>

Patients with behavioral health disorders frequently access medical care through the hospital's emergency department. Psychiatric emergency department patients continue to suffer the greatest delay in access to inpatient beds. In New South Wales, Australia, the Mental Health Intervention Team reports that from 2000 to 2007, behavioral health incidents have increased by 1,265 or 45.27% each year.<sup>15</sup> Although this increase would be

considered excessive for most states and countries, the reduced number of available inpatient psychiatric beds has created a difficult problem—behavioral health patients not being transferred out of the emergency department in a timely manner. Many emergency departments have had to learn to provide a level of care for these patients long after their psychiatric evaluation and medical clearance. Behavioral health patients are now often spending days, not hours, in the emergency department. This is overwhelming many emergency departments, as behavioral health patients often need one-on-one supervision. The escalated amount of tension often created by these anxious patients frequently results in a larger role for security staff to have a greater involvement with the behavioral health patient.

For the few healthcare organizations that continue to offer inpatient behavioral health services (approximately 27% of hospitals in the United States),<sup>16</sup> a call to the security department generally indicates that an urgent situation exists and that additional help is required to deal with the problem. Unlike past years when security officers rarely responded to the mental health unit, today, the typical procedure is for uniformed officers to respond as they would to any other call for patient support. The rationale for this response is that mental health treatment should provide experience and therapy so that the patient will be able to function in society. In society, someone who causes a disturbance should expect the authorities to be called.

Armed officers, as opposed to unarmed officers, should use a different response to problems in the mental health unit. Each HCF must develop its own approach. In one large facility, the first security officer to arrive waits outside the unit and collects equipment from the other officers who respond. Other hospitals have installed gun lockers just outside the unit. Of course, circumstances will prevail, and in a nonmedical emergency, such as a fire or major accident, a different response is indicated.

As a general rule, security officers do not patrol mental health units. Regular medical care personnel provide surveillance and control of patients and visitors as part of their routine activity. However, security may be part of the access control system for locked units and they may also be required to patrol the unit under special circumstances.

Elopement is always a concern when treating the mental health patients. It is reported that 3–15% of all patients admitted to mental health units elope each year. Certain sources suggest that there are identifiable characteristics of the patient who is prone to elope. Such sources indicate that these patients are generally male and usually verbalize a desire to leave prior to elopement. Often they have eloped on prior occasions and have a diagnosis of schizophrenia or a mood disorder.<sup>17</sup> Security and the mental health unit staff must work closely with each other to manage the preventive aspects of elopement.

## Patients with Autism

The rate of autism has grown 10-fold since the late 1990s. The Centers for Disease Control Prevention estimates that 1 in every 150 children is believed to have some form of autism. Throughout the world, the number of people diagnosed with autism is growing, showing no racial, ethnic, or social boundaries.<sup>18</sup>

Children and adults with autism now live, work, go to school, and recreate in the community. They also frequently present themselves to the healthcare organization as a patient or a visitor. Healthcare security officers have interactions with children and adults with autism, their parents and care providers. Research indicates that individuals with autism and other developmental disabilities are approximately seven times more likely to come in contact with security professionals than are members of the general population.

Healthcare security officers should understand the nature of autism and be trained to manage situations involving patients with this condition more effectively. Security staff can use the acronym AUTISM shown in Table 12-2 to help them remember the methodology they should use when dealing with individuals with autism.

Healthcare security officers may unexpectedly encounter or be asked to find a person with autism. The information may be learned from a security dispatcher, someone at the scene, or from the person directly. Recognizing the behavior symptoms and knowing contact approaches can minimize situations of risk—risk to or victimization of the person with autism, as well as risk to the security officer. Dennis Debbaudt, a professional investigator and law enforcement trainer, and proud father of a young man with autism, has developed some specific tips for healthcare security officers responding to patients with autism:

**Table 12-2** Security Officer Response to Autistic Patients

Security Officer Response to Autistic Patients	
A	<b>Approach the person in a quiet, nonthreatening manner.</b> Because people with autism may be hypersensitive to stimuli, officers should attempt to avoid quick motions and gestures that a person with autism may perceive, even remotely, as threatening.
U	<b>Understand that touching an individual with autism may cause a protective “fight or flight” reaction.</b> Officers should never touch the individual on the shoulders or near the face. Autistic hypersensitivity includes being touched and even extends to invasions of their personal space.
T	<b>Talk to the person in a moderate and calm voice.</b> Although officers may have to repeat their directions or questions several times, they should be patient and wait for answers. Speaking loudly will not help and may even be viewed as threatening.
I	<b>Instructions should be simple and direct with no use of slang.</b> An autistic patient will take an officer’s statements literally. “Do you think that’s cool?” or “Up against the wall!” probably will cause confusion and result in an inappropriate or unexpected response. Officers should use specific commands, such as, “stand up” or “go to the car, now” to reduce the chance of confusion.
S	Seek all indicators to evaluate the situation as it unfolds.
M	Maintain a safe distance until any inappropriate behavior lessens but remain alert to the possibility of outbursts or impulsive acts. <sup>19</sup>

Source: Courtesy of Dennis Debbaudt.

- Make sure the person is unarmed and maintain a safe distance, because they may suddenly invade your personal space.
- Talk calmly and softly.
- Speak in direct, short phrases such as: “Stand up now” or “Get in the car.”
- Avoid slang expressions, such as: “What’s up your sleeve?” or “Are you pulling my leg?”
- Allow for delayed responses to your questions or commands.
- Repeat or rephrase when necessary.
- Consider use of pictures, written phrases and commands, and sign language.
- Use low gestures for attention; avoid rapid pointing or waving.
- Examine the individual for presence of medical alert jewelry or tags, or an autism handout card.
- Model calming body language (such as slow breathing and keeping hands low).
- Model the behavior you want the person to display.
- A person with autism may not react well to changes in routine or the presence of strangers, even a uniformed stranger.
- Security officers should not interpret the person’s failure to respond to orders or questions as a lack of cooperation or a reason for using increased force.
- Seek information and assistance from a parent or others at the scene about how to communicate with and de-escalate the person’s behavior.
- Avoid stopping repetitive behaviors unless there is risk of injury to yourself or others. If the individual is holding an inanimate object and appears to be fascinated with it, consider allowing him or her to keep the item for the calming effect (if safety is not jeopardized).
- Evaluate for injury. The individual may not ask for help or show any indication of pain, even though injury seems apparent.
- If possible, turn off sirens and flashing lights and remove canine partners, crowds, or other sensory stimulation from the scene.
- If the person’s behavior escalates, use geographic containment and maintain a safe distance until any inappropriate behaviors lessen.
- Remain alert to the possibility of outbursts or impulsive acts.
- Use your discretion. If you have determined that the person is unarmed and if you have established geographic containment, use all available time to allow the person to de-escalate himself/herself without your intervention.<sup>20</sup>

## The Forensic Patient

The forensic patient continues to be both an issue and challenge for the healthcare security administrator. At any given moment, there may be prisoners inside an HCF. Outside of the courtroom, the hospital is the only other public place that experiences such large volume of prisoner visits.

Among the challenges are the different players who become involved in the treatment, care, and custody of the patient. It begins with the requirement to provide treatment and

security protocol training for forensic staff (police, sheriff, correctional officers, etc.); security assessment of the safety and security of staff and patients relative to the resources being provided by the forensic staff; providing information to the facility security operations staff; being cognizant of TJC and Centers for Medicare & Medicaid Services restraint and seclusion issues; and coordination between security operations and the custody authority/agency.

The forensic patient may either be brought to the medical care facility for emergency or outpatient treatment or for a planned hospitalization as an inpatient. In all the cases, the forensic patient must be viewed as a potential threat to the facility. The typical HCF does not host an environment that is well equipped or prepared for management of forensic patients. Most healthcare organizations do not have holding cells or other security protocols commonly found in the jail or corrections facility. Joel Lashley of Children's Hospital of Wisconsin in Milwaukee claims that "a typical hospital is the only unprepared environment that is an integral component of the criminal justice system. Corrections officers receive scant training to prepare them for the clinical setting, which is why officers, bystanders and medical personnel are often hurt and even killed by prisoner patients. It's also a reason so many inmates escape from hospitals."<sup>21</sup>

A growing security issue is that the number of serious security/criminal incidents involving forensic patients in the HCF has escalated over the past decade. It is projected that the number of forensic patients being treated in HCFs, outside of detention centers, will continue to increase as the number of prisoners continues to increase. The US correctional population in 2006 numbered 2.2 million according to the Department of Justice's Bureau of Justice Statistics and this number is expected to increase each year into the foreseeable future.<sup>22</sup> Add to this the number of forensic patients, under arrest or held under court order, who have not yet been entered into the correctional system.

An added security dimension associated with this type of patient is due to a very questionable practice on the part of law enforcement. This practice occurs when a police officer discovers that an arrested person will be in the hospital for a number of days, and, therefore, "un-arrests" the patient to avoid the time and expense of furnishing a 24-hour guard of the patient. In these cases, the police ask the healthcare provider to advise them on the planned discharge of the patient so that they can show up and rearrest the individual. In other cases, the arrested patient is simply issued a citation to appear in court.

Confusion and conflict can take place when caring for the forensic patient. Law enforcement or correctional personnel often do not understand the procedures of medical care, while medical care staff do not always understand the implications of the custody of the patient. Most correctional agencies will call ahead before just arriving with the forensic patient. However, the location of where medical service is provided is often unpredictable and based on the need of the patient. The forensic patient may initially access care through the emergency department, but is often found in surgery (pre-op, post-op, and/or recovery), MRI, radiology, the behavioral health unit, and, from time-to-time, the maternity unit.

Many healthcare organizations have a predetermined access point into their facility, often the ambulance bay, for forensic patients and correctional staff to help ensure



the safest entry into the facility that causes the least amount of disruption. To minimize the negative perception often created by having forensic patients in the HCF staff, security staff often greet the correctional team with a wheelchair and blanket to conceal their restraints and prisoner status.

It is important that the prisoner remain in the custody of the correctional officer at all times to include being properly shackled to the wheelchair or gurney. Forensic patients have seriously injured and killed correctional officers by kicking them from gurneys.<sup>23</sup> Medical care staff should never ask to remove restraints unless medically required. Sometimes handcuffs, belly chains, and shackles must be removed for MRI imaging procedures, X-rays at the restraint site, or other procedures that may genuinely be incompatible with standard police restraints. An alternative restraint should always be added to include temporary use of medical restraint devices if necessary. If this is not possible, the healthcare organization should require more than one correctional officer to assist in managing unrestrained forensic patients. Managing unrestrained prisoners alone in any environment is inherently dangerous and should not be tolerated.

Platte Valley Medical Center in Brighton, CO, learned a difficult lesson after a forensic patient was shot in their hallway after a failed attempt to escape. The correctional officer, required to remove the restraint devices so that X-rays could be taken at the restraint site, positioned himself behind lead shielding at one of two entrances to the room. The prisoner, sensing the opportunity to escape, fled the room and did not obey instructions, from the officer to stop. The correctional officer shot the prisoner. The after action review revealed that the officer's action was appropriate; however, further investigation by the hospital and the correctional agency revealed that a second officer could have prevented the situation altogether as the unrestrained prisoner would have been outnumbered.

TJC also views forensic patients—especially those patients who are shackled to their beds—as being at some risk should there be a fire or other emergency situation. The commission has issued a compliance standard regarding the training of guards for forensic persons. This standard can be found in the Human Resources section of the accreditation manual. The current TJC standard (H.R.2.10, EP 10) requires that any person guarding a forensic patient receive orientation and education on how to interact in the medical care setting, on procedures for responding to unusual events (fire, disasters, medical emergencies), on proper channels of communications, and on the distinction of the administrative/clinical restraint/seclusion elements of control.

There are a number of ways to accomplish this training. The most common method is to furnish written information to the forensic staff (guard) upon admission of the patient. In this method, the first guard is asked to make this information a part of the agency's post orders and to pass on the information to all other guards.

A rather unique program developed for training law enforcement agencies in guarding inpatient prisoners was developed jointly by three hospital systems in Brevard County, FL. This program, spearheaded by Jim Kending of Health First in Melbourne, FL, consisted of developing a 10-minute video relative to guarding the forensic patient. This video was distributed to some 20 area criminal justice agencies to be used as a roll-call

training activity. The video is also being utilized by the Brevard County law enforcement and corrections academy in their recruit training program. A standardized orientation guide and acknowledgment form is also used with each correctional facility.

The safety of patients and healthcare personnel is a priority. Defining roles in the treatment of inmates and arrestees is especially important. [Figure 12-6](#) provides a list of the duties that the hospital will take pertaining to forensic patients.<sup>24</sup>

[Figure 12-6](#) lists the duties of a hospital pertaining to forensic patients in the inpatient setting (courtesy of *Environment of Care News*, reprinted with permission).

Most hospitals do not have secure prison wards or units and are often not prepared to care for forensic patients. IAHSS provides some general guidelines that should be taken into consideration by all hospitals that admit forensic patients.

#### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.03

##### **Forensic Patient Security**

**STATEMENT:** Healthcare facilities (HCFs) that treat forensic patients (prisoners) will develop a multidisciplinary process for providing appropriate security measures.

##### **INTENT:**

- a. The forensic plan should contain at a minimum, the following:
  1. An HCF employee be identified to coordinate the protocols with the law enforcement and corrections agencies that present patients for medical care.
  2. Forensic staff orientation and education procedures and protocols to include:
    - How to interact with patients; procedures for responding to unusual clinical events and incidents; the HCF's channels for clinical, security, and administrative communication; distinctions between administrative and clinical seclusion and restraint.
    - Forensic patients should be monitored at all times by forensic staff including while in restrooms and during clinical procedures.
  3. Provide clinical staff orientation to the Forensic Policy.
  4. Procedures to minimize or eliminate weapons or potential weapons in close proximity to forensic patients especially in enclosed spaces (e.g., bathrooms, elevators, treatment rooms, etc.).
  5. Forensic restraints:
    - The types and numbers of restraint devices to be used should be identified.
    - Unless clinically contraindicated, forensic restraints (handcuffs and/or leg irons) should be used at all times for all guarded forensic patients.
    - Consider other methods to minimize the need to remove restraints such as the use of a portable commode chair.
  6. Procedures for notifying appropriate departments upon the arrival of forensic patients at the HCF. It is recommended the Security Department conduct an initial

risk assessment and facilitate the case-specific communication between clinical and forensic staff.

- b. Security should maintain a log of forensic patients treated. Incidents involving forensic patients and staff should be documented, tracked, trended, and evaluated by an appropriate security administrator.
- c. Evaluate physical security for the primary locations forensic patients are treated. Emergency care, inpatient, and clinic spaces are locations to consider. Assess entrances points for prisoner patients: evaluate security measures in place in each area and consider designating entry points versus allowing random access points. Consider designating a room or holding area so prisoner patients can be thoroughly searched and cleansed of potential weapons (e.g., unnecessary furniture, medical instruments, pens, etc.) as well as contraband—both before and after use.
- d. Visitors to a forensic patient should be solely at the discretion of the forensic agency in accordance with its policies.

**Approved:** December 2006

**Last Revised:** October 2008

## The Wandering Patient (Dementia and Psychological Related)

Wandering patients are a security concern presented by certain types of dementia patients, most frequently those with Alzheimer's disease. It is estimated that each week at least one resident of the nation's nursing home facilities wanders away from a care facility and dies. The wandering patient situation is of course not limited to nursing homes. The mental health facility and even certain patients in the general medical/surgical category can be wandering patients. Intensive care staff have long recognized psychological responses of patients, which include delirium, catastrophic reaction, and euphoric response. The most common of these responses is delirium, which has been described on a range from slight clouding of consciousness to a full-blown psychotic reaction. In this respect, patients experience varying degrees of cognitive impairment.

A patient movement control system utilizing an electronic tag is a fairly common safeguard for suspected wandering patients. The patient wears a tag that contains a radio frequency circuit; this circuit communicates with a detection sensor usually installed at the exit door or elevator opening. Some systems do not use multiple-detection sensors at doors, but have a radio receiver installed at a central location instead. In these systems, the distance between the tag and central monitor is constantly measured with an alarm, which sounds when a predetermined distance is exceeded. Electronic systems can be installed as stand-alone systems at each door or as centralized computer-controlled systems. Computerized systems are capable of identifying the individual patient and can display the alarm information as either text or a graphic map. Individual tags can

### Forensic Patient Protocol: Duties of Hospital (Inpatient Setting)

1. The hospital's Security Department shall conduct an orientation, including a review of the elements of performance for Standard HR.2.10, to any law enforcement guarding an in-custody arrestee or jail inmate.
2. The hospital will provide a safe "finger meal"\* to the in-custody arrestee or jail inmate (e.g., sandwich, milk carton consistent with the medical condition(s) present).
3. The hospital shall provide a meal to the law enforcement officer or corrections officer and invoice the agency accordingly.
4. The hospital shall provide a private room (when available) for the in-custody arrestee or jail inmate.
5. The phone shall be available in the room and is to be used only by the law enforcement or corrections officer in attendance.
6. There will be no visitation allowed for any in-custody arrestee or jail inmate.
  - a. Exceptions to be approved by the Commander of the Jail or municipal police agency (or designee) and the Chief of Hospital Security for consultation with a lawyer or end-of-life situation and other approved situations.
  - b. Exception for juveniles: parent(s) or guardian(s) are permitted to visit.
7. The hospital's Security Department will provide a bathroom break for the law enforcement or the corrections officer guarding the patient and observe the patient during this brief time period, as needed.
8. The hospital's shift lead security representative shall travel to the in-custody arrestee's or inmate's room on each shift and introduce him- or herself to the law enforcement or corrections officer.
9. The hospital Security Department shall provide a department radio (to the law enforcement or corrections officer guarding the patient-prisoner or in-custody arrestee) to provide priority communication capability. Follow-up appointments and discharge instructions will be provided to the law enforcement officer or corrections officer guarding the patient only.
10. The patient's medical needs (including toileting) shall be the responsibility of the clinical employees of the hospital.
11. The hospital will not disclose any information, including room assignment, to walk-in visitors and/or incoming telephone inquiries, pertaining to a guarded patient. The only exception to this is for the parents or legal guardian who comes to the hospital to visit the juvenile patient.

\*Finger meal means food is eaten with the fingers, since no utensils are allowed.

**FIGURE 12-6** Forensic patient protocol: Duties of hospital (inpatient setting) (Bowers, D. M. (1999). *Journal of Healthcare Protection Management*, 15(1), 109–117.).

be deactivated in a number of ways to allow family or staff to take a patient out of the defined secured area.

A rather extensive radio frequency tag system for managing long-term care patients is currently being used at the Sunnybrook Health Sciences Center, which is

part of the University of Toronto (Canada). The Sunnybrook Health Sciences Center is a 1,300-bed facility, with 550 beds being occupied by long-term care patients. There are, thus, varying degrees of control depending on the unit and types of patients. In addition to the radio frequency system, the hospital has what they refer to as the “Blue Shirt Program.” In this program, the at-risk cognitively impaired patients wear a blue shirt with the Sunnybrook Health Sciences Center logo emblazoned in yellow across the back. All staff members—and even members of the immediate community—are educated on the Blue Shirt Program and are asked to report any observed wandering patients.<sup>26</sup>

An effective approach to managing the problem of wandering patients requires proper facility design and physical security safeguards, good control policies and procedures put into practice by staff, and ongoing staff training in the management of the wandering patient.

## The Infant and Pediatric Patient

A great deal has been written about preventive steps that can be taken to avoid the abduction of newborn infants. A facility birthing unit is generally classified as a security sensitive area in terms of TJC compliance standards. As such, the security issues surrounding the abduction of infants will be more fully addressed in *Chapter 20, Security Sensitive Areas*.

The possibility of discharging an infant to the wrong parents is a concern that requires proper clinical management. Security is not often involved in developing clinical policies and procedures, but may well become involved should an actual event occur.

The pediatric patient presents several security risks, including the possibility of abduction, elopement, and the recipient of physical abuse while in the hospital. In addition, pediatric patients may wander off the unit. The possibility of abduction is somewhat higher for the pediatric patient than the newborn infant. This higher risk is the result of a greater length of stay, generally fewer security precautions, and the number of custody battles that involve children. In pediatric abductions, the perpetrator is almost always known, and in many cases there is significant early warning that allows proactive security measures to be put in place.

In recent years, medical care providers and healthcare security administrators have become more and more aware of a form of child abuse referred to as Munchausen by Proxy Syndrome (MBPS). It is a form of child abuse wherein a parent (usually the mother) intentionally manufactures illness in her child and repeatedly presents the child for medical care, disclaiming knowledge as to the cause of the problem. Child victims of MBPS are at risk for serious injury or death. The security department therefore plays a critical role in investigating and managing MSBP. The following are the “symptoms” of MBPS:

- Illness in a child that is simulated (faked) or produced by a parent or other caretaker or both.

- Presentation of the child for medical assessment and care, usually persistently, often resulting in multiple medical procedures.
- Denial of the knowledge by the parent as to the cause of the child's illness.
- Subsiding of acute symptoms and signs when the child is separated from the parent.

Typically, but not always, the mother spends a good deal of time in the hospital with the child and exhibits a remarkable familiarity with medical terminology. She may be “confidentially friendly” with the healthcare staff, although she may show frustration with her child's chronic illness and anger at the medical staff's inadequate vigor in pursuing her child's problems. She may insist that she is the “only one” for whom the child will eat, drink, or swallow medicines. The syndrome often persists for years and can result in death. According to experts, common conditions and symptoms that are created or faked by parents or caregivers with MBPS include failure to thrive, allergies, asthma, vomiting, diarrhea, seizures, and infections.<sup>27</sup>

Bonnie Michelman, CHPA, CPP, Director Police and Security at Massachusetts General Hospital in Boston, and a leading security expert in MBPS, suggests that a multidisciplinary child protection team should become involved the moment MBPS is suspected. The team should include medical personnel, security management, the primary care nurse, social services, mental health professionals, and an epidemiologist (a person who, in part, specializes in figuring out the cause of a disease). Together they must determine whether the child's medical condition can be attributed to MBPS, warranting civil proceedings to remove the child from the perpetrator's care and, possibly, criminal proceedings. Police and security personnel should become involved early in the case, collecting evidence, making timely arrests, and helping to develop a case for prosecution. Once the child is assumed to be at risk, a customized protection plan for the child must be designed and implemented.

## Patient Property

A highly visible and troublesome security problem is missing patient property. The average financial loss is quite small; however, large losses do occasionally occur. The impact of property loss on a sick patient and the negative public relations that result indicate a concern far more important than the value of property involved.

Most hospital facilities engage in a program commonly referred to as preadmission registration, which obtains certain information from the patient before admission. The preadmission information, or instruction, form should state that the hospital does not have adequate storage for personal property and should instruct the patient to leave jewelry, wallets, radios, and similar items at home. The statement should also note that the hospital cannot be responsible for personal property brought to the facility by the patient or brought to the patient by visitors. Bold type should be used to highlight this policy.

When patients are admitted, the person who signs the admissions form should be required to initial a statement that the hospital is not responsible for personal property

not in its possession or control. The patient should be advised to surrender for safekeeping any keys, credit cards, jewelry, watches, and money over an established limit. There have been numerous instances in which a patient's purse has been stolen from the bedside or closet and the keys and identification used to commit a burglary of the patient's home. A growing number of hospitals have installed hotel-style safes in each inpatient room that allows for patients to provide for the security of their valuables in their room. These styles of safes should be properly secured inside the room and be of sufficient strength to withstand a serious attempt at breaking in or removal from the area. These safes should only be used by patients who are lucid.

### General Principles for Handling Patient Valuables

Property being checked with the hospital requires a sound handling procedure. Hospital security administrators should check the following principles against their current procedure:

- The patient valuables envelope should be tamper proof. A heavy, numbered envelope should be used, which, when sealed, must be torn open to remove the contents.
- All information regarding the contents of the envelope should be on a separate sheet placed in the envelope, signed and sealed in front of the patient. There should be nothing on the exterior of the envelope indicating the contents of the envelope except patient name, bag number, and room number.
- A minimum of two witnesses should verify and document what goes into the patient envelope including the patient. If the patient is not lucid, the witnesses should personally observe the valuable being placed in the envelope and the envelope being sealed.
- An accountability log should be kept documenting the Date, Time, Patient Name, Room Number, Bag Number, and Witness Names. The property stored in the envelopes should not be listed on this record. Stored inside the patient valuables lockbox, each envelope should be inspected and inventoried when shifts change.
- The lockbox should have a double lock and key mechanism, and regardless of the circumstances, always require two people to gain entry at all times. The lockbox should be bolted to the floor and be of sufficient strength to withstand a serious attempt at breaking in or removing the lockbox from the area.
- When valuables are released, confirmation that the contents of the envelope are intact should be always be made. Discrepancies noted on a security incident report and be immediately investigated. If the patient is deceased, the patient valuables should not be released until proper verification can be made of the person taking possession of the valuables (authorized next of kin or has power of attorney).
- When the patient requests the partial withdrawal of property, a new envelope and receipt should be prepared, and the number of the original envelope and the original receipt included.

Regardless of how well admissions personnel perform their job, some patient will always end up with too much personal property in the room. The nursing staff should assume some responsibility to reduce this vulnerability. They should encourage the patient to send property home or to permit the hospital to hold the property for safekeeping. Otherwise, an admission clerk must respond to the unit; in some cases, the responsibility is assigned to the security department to obtain the property and transport it to the safekeeping area.

Outpatient property can also present security problems. Outpatients are presumed to be better able to care for their property than inpatients. Small signs in clothes-changing areas should indicate that the organization is not responsible for lost or missing property. Many outpatient facilities provide individual lockers for their patients to secure personal property during the outpatient procedure.

Hospitals should deny all claims for missing property that was not held by the hospital. Weak-hearted administrators or risk managers who pay these claims will find that a monstrous and costly situation may develop. Each claim must always be evaluated on its own merits.

## Visitors

In contrast to limited patient contact, security officers will often initiate contact with visitors, vendors, and suppliers. In regulating parking, loading docks, ambulance entrances, and building access, security officers take on the task of regulating visitors. Once visitors reach their intended destination, such as a patient room or the outpatient department, the regulating task is transferred to the facility personnel responsible for the specific work area or unit.

In all contacts, whether with a patient, visitor, or employee, security staff must bear in mind that they are representatives of the healthcare organization. They must make every effort to ensure that their interactions are carried out with tact and diplomacy. Security officers are often the first people encountered upon entering the healthcare system. Impressions made at this point are lasting, and security officers should capitalize on this opportunity to act professionally.

It is generally agreed that sick or convalescing patients need visitors as part of the recovery process. On the other hand, visitors can interfere with medical care, refuse to leave when asked, steal, complain, sleep in patient rooms, litter, engage in loud and boisterous conduct, and leave patients exhausted or in a state of tension, which can be detrimental to the patient's recovery process.

Many factors affect visitor control. Chief among them is the philosophy of the administration. The philosophy of patient and family-centered care is espoused by a growing number of healthcare administrators who feel that families should be a part of the care giving process. Thus, visiting the facility is the right of the family and should not be controlled or discouraged. Other administrators feel that good patient care requires strict visitor control. The trend in healthcare continues toward more liberal visiting policies.



However, today, there is a noticeable shift toward greeting all visitors who enter the facility, and restricting access to the facility after hours only to those who have a specific need.

A second major factor affecting visitor control is that the poor layout and design of many HCFs greatly hinder meaningful visitor control, at least in terms of the cost to overcome the design deficiency.

Areas of the hospital that present special visitor control considerations are the medical/surgical patient units, pediatric units, obstetrical units, behavioral health units, ICUs, the medical treatment area of the emergency department, and isolation units. The discussion here focuses on the overall visitor control problem because these specialty units generally rely on their own procedures and unit personnel for control.

Some people question whether visitor control rightfully belongs in the realm of security operations. This view may have merit when the concern is for legitimate visitors during designated visitor hours. However, overall access control that includes visitors during late-night hours is a protection responsibility.

An adjunct to access control is the questioning of persons, including visitors and employees, who appear to need help, or persons who are acting or looking suspicious. People who are stopped by security and questioned concerning their business can often become annoyed or hostile regardless of the approach or intent of the security officer.

## Time Periods

To properly view access control, two distinct time periods, each presenting different security ramifications, should be considered: designated patient visiting hours and after normal operational hours.

### *Designated Patient Visiting Hours*

The time designated by the facility for visiting patients can vary. Many healthcare organizations have dispensed with visiting hour altogether and have no restrictions for the designated time for visiting patients. Most hospitals remain traditional and still define specific hours for visiting patients. Specialized units, such as the ICU, are often more restrictive, limiting the number of visitors, placing minimum age restrictions for the visitor with a predetermined maximum length for an individual visit (or in aggregate). Other specialized units, such as the Pediatric Unit, are often more liberal, allowing for and often encouraging parents to remain in the patient's room for the duration of the patient stay.

The majority of hospitals do not issue specific visitor identification during regular visiting hours. For those that do, the general procedure is to prepare a temporary, self-expiring badge for each visitor. These passes are issued when the visitor enters the facility. Technology advances have allowed for the self-adhesive badge to be produced automatically from a government-issued identification card and screened against a database of known sex offender registries or against organizationally generated no visitor (stop) lists. Facial recognition software used at Exempla Saint Joseph Hospital in Denver, CO, has expedited the time it takes to issue the visitor badge and providing a comprehensive

database that helps the hospital readily identify visitors who have previously created problems for the hospital, its patients, staff, or other visitors.

The details of most visitor management systems can be tailored to meet a facility's specific needs. Most facilities use a self-adhesive disposable badge, while others use a reusable laminated visitor badge. A growing number of facilities custom-make badges for visitors using PCs and video-imaging techniques. A few organizations have sold advertising on the badge to offset the expense associated with the system.

Badge and pass systems can work; however, numerous elevators and stairwells leading to patient units can tempt visitors to bypass the entire system. A visitor control plan used during regular visiting hours should be considered as minimal protection for the patient and only as a screening procedure at best.

Regardless of the procedures used, the ultimate responsibility for patient visitor control must remain with the personnel assigned to the patient care units. They must determine whether a patient has too many visitors, or whether the visitors will have an adverse effect on the patient or the facility as a whole. A nurse or nursing assistant can generally correct undesired visitor actions without adverse public reaction. If unit personnel cannot resolve the problem, a security officer may then be called for support.

#### *After Hours*

A system of after-hours visitor control should be established even if there is an open visiting policy. All people entering the HCF after hours should be greeted, their purpose for entering the facility established, and their entry into the facility authorized.

The legitimate need for after-hours visitation is limitless: whether it is the person who is leaving town and wants to visit before leaving or the out-of-town visitor who was delayed and could not get to the facility during regular visiting hours. These and other extenuating circumstances must be managed in the visitor control plan.

What is believed to be after hours will vary among hospitals. Most HCFs close down after visiting hours, but many unlock various entrances and exits for shift changes in the absence of electronic locking systems, providing controlled employee access points. Regardless of the patient visiting hours philosophy in place, the HCF should control access to all doors providing uninhibited access into the facility after normal operating hours. This should include access connections from physician office buildings to the hospital proper along with connected parking decks. These connecting corridors usually have a major entrance, which provides a good access point for affecting an element of control.

During this period, the entire complex should be locked, channeling patients and visitors to one designated entrance where a visitor control person is in attendance. Most often the designated after-hours entrance is the emergency department. In facilities that do not provide emergency care service, it is generally the main entrance. All general-use doors available during the operational period should have signs directing the public to the designated night entrance when these general-use doors are locked.

In many facilities, all entrances are locked, and controls vary from electronic door controls, to video surveillance, to security officers. Obviously, the integrity of the access control system can be compromised by many means. Compromises can occur when a visitor or employee opens an exit door to permit entry for someone on the outside and when exit doors do not latch properly. Security patrols and alarm hardware at emergency exit doors are helpful in preventing breaches of the security system.

To properly identify authorized visitors to the facility after hours, most healthcare organizations incorporate a system of visitor badging. After a person is cleared for access, the date and destination can be written on the badge. A log should be maintained that includes name, time, destination, purpose, patient to be visited, and the visitor's signature. The signature is helpful psychologically because it implies stricter control. In some control programs, personal identification, such as a driver's license or other form government-issued identification, must be presented; however, this requirement is somewhat superfluous as legitimate visitors will not be denied entry just because they cannot produce such identification. If such identification is an element of the access control program, the badge itself should not be held by the facility to be returned upon exiting.

The access control point should be supplied with resource data. A computer database listing all patients and any visitation restrictions, such as "no visitors," "family only," and "wife may visit anytime" is a common and useful resource.

When a patient's condition deteriorates, the physician often asks the family to come to the facility. Unit nursing personnel are almost always aware of this situation and should notify the public access control point so that access can be expeditiously handled. It is poor public relations when family members have been called and are unnecessarily delayed because no one notified the person at the control point.

It is not uncommon for someone who requires emergency room treatment to arrive with numerous friends or relatives. Because treatment is not instantaneous, these visitors often desire to leave the waiting area to explore for food or other amenities. Many organizations manage this need by developing a controlled set of locked doors leading from the emergency department waiting area equipped with an electrical release system managed by the security officer responsible for after-hour access control. Thus, the officer is aware of who is granted access into the facility. The proper layout and design of the emergency department is covered in *Chapter 20, Security Sensitive Areas*.

One of the pitfalls of an after-hours badging program is legitimate visitors who enter the facility during regular visiting hours when no pass or badge system is in effect. If they are given permission by unit staff to remain after visiting hours or even for the entire night, the charge nurse should be required to send them to the access control point for badging. In this way, all late-night visitors will be badged—not just those entering after the night-access control system goes into effect. In some programs, security officers make the rounds of patient floors with hand-held machines to produce the visitor badge.

All access control personnel must exercise extreme caution, so that legitimate access to the facility is not denied. A person who appears to be intoxicated may be a diabetic in shock seeking medical care.

## Large Acreage Facilities

Visitors to HCFs with extensive grounds (often public/government-owned facilities) can be effectively controlled at a single vehicle entrance. These facilities generally have some form of perimeter barrier, and all traffic can be channeled through a central access control point. Most control systems record the visit on a log and issue a pass to be displayed on the dashboard of the vehicle. The pass is retrieved when the vehicle leaves. This system of vehicle access control does not preclude another system of visitor control at any of the units within the perimeter.

All medical care facilities require a system of visitor control tailored to the specific needs of their facility. Systems cannot simply be transplanted; however, a review of other hospital visitor control programs can help to eliminate the pitfalls that may jeopardize a new or reorganized visitor control program.

## References

1. The Johns Hopkins Hospital. (2009). *Patient bill of rights and responsibilities*. Retrieved May 3, 2009, from [http://www.hopkinsmedicine.org/the\\_johns\\_hopkins\\_hospital/patients/rights.html](http://www.hopkinsmedicine.org/the_johns_hopkins_hospital/patients/rights.html).
2. Gerardi, D. (2007, December). *Elopement*. Retrieved May 1, 2009 from <http://www.webmm.ahrq.gov/case.aspx?caseID=164#ref4>.
3. UPMC has new procedure to find missing patients. (2009, January 3). *Pittsburgh Post-Gazette Now*. Retrieved January 3, 2009, from <http://www.post-gazette.com/pg/08365/938554-100.stm>.
4. Extra security call as patients go missing. (2007, October 17). *Surrey Times Online*. Retrieved June 25, 2009, from [http://www.getsurrey.co.uk/news/s/2016475\\_extra\\_security\\_call\\_as\\_patients\\_go\\_missing](http://www.getsurrey.co.uk/news/s/2016475_extra_security_call_as_patients_go_missing).
5. DeRosier, J. M., & Taylor, L. (2005). Analyzing missing patient events at the VA VA National Center for Patient Safety, Retrieved May 3, 2009, from [http://www.va.gov/ncps/TIPS/Docs/TIPS\\_NovDec05.pdf](http://www.va.gov/ncps/TIPS/Docs/TIPS_NovDec05.pdf). *TIPS (Topics in Patient Safety)*, 5(6), 1–2.
6. The Joint Commission. (2005, October). Sentinel event policy and procedures. Retrieved December 31, 2008 from [http://www.jointcommission.org/NR/rdonlyres/F84F9DC6-A5DA-490F-A91F-A9FCE26347C4/0/SE\\_chapter\\_july07.pdf](http://www.jointcommission.org/NR/rdonlyres/F84F9DC6-A5DA-490F-A91F-A9FCE26347C4/0/SE_chapter_july07.pdf).
7. The Joint Commission. (2008). Sentinel event statistics. Retrieved December 31, 2008, from <http://www.jointcommission.org/SentinelEvents/Statistics/>.
8. National Center for Public Safety. (2009, March 4). VHA NCPS escape and elopement management. Retrieved May 3, 2009, from <http://www.va.gov/ncps/CogAids/EscapeElope/index.html>.
9. Gerardi, D. (2007, December). *Elopement*. Retrieved May 1, 2009, from <http://www.webmm.ahrq.gov/case.aspx?caseID=164#ref4>.
10. IAHSS. (2009). Legal actions against your strip search policies for ER patients with psychiatric problems. *Healthcare Security and Safety Directions*, 22(2), 11–12.
11. Schoolfield, D. (2008). Evaluation of very important person (VIP) policy to include victims of violence. *Journal of Healthcare Protection Management*, 24(2), 88–89.
12. American College of Emergency Physicians. (2008, April). Protection from physical violence in the emergency department environment. Retrieved May 9, 2009, from <http://www.acep.org/practres.aspx?id=29654>.

13. American Hospital Association. (2007, September). Behavioral health challenges in the general hospital: Practical help for hospital leaders. *Behavioral Health Task Force Report*, p. 1.
14. American Hospital Association. (2007, September). Behavioral health challenges in the general hospital: Practical help for hospital leaders. *Behavioral Health Task Force Report*, p. 1.
15. Donohue, D. (2008, November 27). *Multi-agency collaboration for healthcare security risks: A presentation*. Presented at the Australian Hospital and Healthcare Security and Safety Conference.
16. American Hospital Association. (2007, September). Behavioral health challenges in the general hospital: Practical help for hospital leaders. *Behavioral Health Task Force Report*, p. 3.
17. Iatts, W. E. (1998). Psychiatric patients: Promises liability and predicting patient elopement. *Journal of Healthcare Protection Management*, 14(2), 75.
18. Debbaudt, D. (2009). Patients with autism and other high risks: A growing challenge for healthcare security. *Journal of Healthcare Protection Management*, 25(1), 15.
19. Debbaudt, D., & Rothman, D. (2001). Contact with individuals with autism: Effective resolutions. *FBI Law Enforcement Bulletin*, 7(4), 20–24.
20. Debbaudt, D. (2009). Patients with autism and other high risks: A growing challenge for healthcare security. *Journal of Healthcare Protection Management*, 25(1), 19.
21. Lashley, J. (2009, March 10). Treatment, care and custody: Securing the hospital environment. *CorrectionsOne News*. Retrieved March 11, 2009, from [http://www.correctionsone.com/pc\\_print.asp?vid=1778372](http://www.correctionsone.com/pc_print.asp?vid=1778372).
22. Gonzalez, F. (2008, January). Corrective action: Corrections security team delivers leading edge technology. *Security Products Magazine*. Retrieved June 25, 2009, from <http://secprodonline.com/Articles/2008/01/03/Corrective-Action.aspx>.
23. Lashley, J. (2009, March 10). Treatment, care and custody: Securing the hospital environment. *CorrectionsOne News*. Retrieved March 11, 2009, from [http://www.correctionsone.com/pc\\_print.asp?vid=1778372](http://www.correctionsone.com/pc_print.asp?vid=1778372).
24. Safety in treating inmates and arrestees. (2008). *Environment of Care News*, 11(6), 6–7.
25. Bowers, D. M. (1999). Closing the door to wanderers. *Journal of Healthcare Protection Management*, 15(1), 109–117.
26. Partington, G. (1997, November). RF system keep up with long-term patients. *Access Control and Security Systems*, pp. 1 and 23.
27. Munchausen by proxy syndrome (MBPS). (2008, December). Retrieved May 16, 2009, from <http://kidshealth.org/parent/general/sick/munchausen.html>.

## Public Safety Liaison

Healthcare organizations must ensure that they provide proper medical care to patients while protecting the legal rights of patients and expediting the legitimate activities of public safety agencies. The primary objectives of healthcare organizations and of public safety agencies can be quite different with respect to patients. The relationship of the patient to the law enforcement agency determines the procedure to be followed. In other words, a patient who is the subject of an investigation, is in protective custody, or is a witness should be handled differently than a patient who is actually under arrest, incarcerated, or for whom an arrest warrant has been issued. Cooperation and understanding of both the healthcare organization and public safety staff are advantageous for both parties. The problems or potential issues between public safety and healthcare employees are less acute; however, objectives and policies must be mutually respected. The majority of interaction between security and public safety agencies is with local and state law enforcement authorities and/or correctional officers. In addition, fire service, emergency preparedness, border patrol, and other federal law enforcement agencies also have frequent business with healthcare organizations. The security department is the primary contact point for these interactions.

### Dynamics of Security and Law Enforcement Liaison

Despite a long history of striving for professional interaction between security and law enforcement, the progress has been slow and often contentious. The identified need for public law enforcement and private security to complement each other in the protection of our society dates back to the emergence of private security following World War II. This need was formalized in the Task Force Report on Private Security (1976), which stated “public law enforcement and private security agencies should work closely together, because their respective roles are complementary in the effort to control crime. Indeed, the magnitude of the nation’s crime problem should preclude any form of competition between the two.”<sup>1</sup> Law enforcement has been slow to embrace the fact that private security has in fact made significant contributions in preventing crime and providing information that has resulted in millions of arrests that would not have occurred through law enforcement efforts alone. The Hallcrest Report II (Private Security Trends) concluded that private security is America’s primary protective resource in terms of dollars spent and the employment of personnel. It is estimated that today there are over two million

people employed in private security, with annual expenditures of over \$60 billion. This compares to approximately 625,000 individuals employed in federal, state, and local law enforcement positions expending some \$40 billion annually.<sup>2</sup>

There have always been exceptions to the lack of significant cooperation between law enforcement and security. Many professional police executives have understood that without private security, their respective geographical entities and the nation as a whole would be overrun by lawlessness. As a general rule, the cooperation has been more effective at local levels and in smaller law enforcement agencies. This is not to say that some larger jurisdictions, such as Dallas, TX, and New York City, have not been in the forefront in organizing and promoting cooperative programs.

It should be noted that there has been an increased understanding by the public as to the definition, role, and contributions of security since the terrorist attack on the World Trade Center. The world of security drastically changed on September 11, 2001. Even with this change, there appear to be various issues that continue to inhibit fostering great progress in the strained security/police relationship. Among these issues are:

- A lack of mutual respect on either side.
- Mutual image and communications barriers.
- A lack of law enforcement knowledge concerning the role and responsibilities of security.
- A lack of standards regarding security personnel.
- Jurisdiction conflict with private organizations relative to corporate theft, computer crimes, drug abuse, etc.
- Moonlighting policies of the police.
- Overlapping areas of responsibility and interest, such as in strikes, traffic control, preserving crime scenes, and investigative activity.
- The erosion of basic police duties being handed over to security (i.e., writing of citations, guarding prisoners, protecting law enforcement facilities) fosters perceived competition. It is projected that police and security operations will work together to a greater extent in the future.
- Law enforcement perceives security personnel as being those who could not meet the standards of police officers in both hiring and training.
- Security perceives police as being overly self-important and somewhat corruptive.
- Law enforcement concern with responding to an inordinate number of false security alarms.<sup>3</sup>

The bottom line is that private security will continue to grow as our law enforcement and judicial systems are unable to provide communities with the level of security and safety that match the needs and desires of business entities and the public.

In some municipal police jurisdictions, private security forces are being utilized to supplement police officers due to shortage of funds, rising crime, and insufficient numbers of police officers. In Oakland, CA, the City Council has recently decided to hire private security for patrol duties in the crime-ridden East Oakland police district.

In Chicago, the City Council is considering a proposal to expand the powers of private security to write traffic citations. In New Orleans it has been proposed to grant special tax incentives to cover the cost of private security for providing neighborhood patrols.<sup>4</sup>

## Police and Security Cooperative Programs

There are numerous formal programs around the country that function to combine police and security information and activities for the good of the community. Most of these programs are at the local law enforcement level; however, there have been some limited state and federal programs aimed at cooperative law enforcement and security endeavors.

**Area Police/Private Security Liaison (APPL):** This organization, founded in 1986 by the New York City Police Department (NYPD) and a number of Security Directors, has grown to become the largest cooperative liaison program between police and security in the nation. Its stated purpose is not only to enhance cooperation, but also to mitigate the credibility gap between police and security. Some of APPL's major activities include

- Monthly and annual meetings;
- Maintain and inventory CCTV business installation to assist in criminal investigation;
- Creation of a specialized crime squad in midtown Manhattan;
- Training for security supervisors;
- Monitoring of security-related legislation;
- Inclusion of security representatives in the NYPD command and control center during specific emergencies.

**Dallas/North Texas Regional Law Enforcement and Security Program:** This program, originally known as LEAPS (Law Enforcement and Private Security), was formed in 1983 and revitalized in 1993. The program functions as a committee made up of the Deputy Chief of the Dallas PD, three security representatives from each of the nine business sectors, and one police officer from each Dallas Police Department division. In addition to general police/security cooperative endeavors, the program provides training of security officers. This training takes place at police substations, giving security officers an increased status and evidence of specific officer training to the satisfaction of police staff.

**Virginia Police and Private Security Alliance (VAPPSA):** This program was created by a group of North Virginia Law Enforcement and security professionals who attended the Federal Law Enforcement Training Center's Operation Partnership program. Sharing of data and monthly meetings are fostering cooperative areas between law enforcement and security.

**Pooling Resources in Defense of Our Environment (PRIDE):** This program is sponsored by the Southfield Michigan Police Department and is not limited to security. It is a business membership of over 150 businesses, including security organizations. A Southfield police sergeant serves as the director of PRIDE, organizing and implementing



its activities. One of the activities to provide a safer place is the training of private security officers who have been granted the authority to enforce parking laws on private property.<sup>2</sup>

### Nassau County Police SPIN Program

Nassau County Police (NCP) Commissioner James Lawrence saw the need for the police and public to share information as part of the NCP strategy to address homeland security, prevent crime, apprehend criminals, and to support business continuity and sustainability after a crisis. The plan that developed was Security Police Information Network (SPIN). Participation in the program is voluntary and limited to security professionals and law enforcement personnel in the New York area. Membership in SPIN is personal and the applicant must complete an application. The information in the application is verified and a criminal history check is completed. In addition to the vetted membership, a community membership has recently been established that allows organizations such as the Chamber of Commerce and Neighborhood Watch groups to receive nonsensitive information.

An important operating concept of the SPIN program is that information is disseminated via e-mail, and recipients are encouraged to reply to the SPIN administrator. The administrator then determines the appropriateness of sharing this information on the SPIN network. Currently, the program continues to evolve and is an important aspect of Nassau County's disaster response and recovery preparations.<sup>5</sup>

### FBI Counterintelligence Domain Project

Yes, government agencies, including the FBI, are beginning to understand that working with the private sector to enhance corporate security is important in promoting national security. Although at present the focus is globalization and the worldwide expansion of business, the nation's healthcare infrastructure is becoming more and more important in the management of terrorist and domestic attacks on the US infrastructure.<sup>6</sup>

### Requests for Law Enforcement Service

A greater demand continues to be placed on security services as traditional law enforcement response becomes less able to answer requests for a physical response. The high cost of law enforcement officers is forcing most communities to alter the method used to respond to requests for nonessential police services. Thus, the police can provide only a minimal amount of investigative support for misdemeanor crimes and many property-related felonies. It is now the standard for victims to report property losses by mail or to go to the police or sheriff's station to report losses. The burden on 911 dispatchers is increasing, and they often must make decisions on whether a physical response is necessary. Professional security programs must respond to scarce law enforcement resources in different ways, including limiting calls for police service to the extent possible. Of course,

pitfalls always exist. When the police are not called as soon as someone would like or when they are not called at all, the action or inaction is often criticized. This criticism comes not only from the population being served, but also from the police agency that wants it both ways. The answer to whether police service was needed in a specific circumstance is often decided after the fact by “Monday morning quarterbacks” who have the benefit of hindsight. Despite this dilemma, the security department must attempt to formulate policies that comply with the local law enforcement methods and procedures of doing business. Often, however, the official administrative protocol is not followed by or reflected in the actions of street officers. Another player is the prosecuting attorney, who may also follow a protocol that is not in complete synchronization with the law enforcement agencies. This situation requires constant liaison with the police jurisdiction involved to avoid misunderstandings.

### Calling for Police Response

General policy should prohibit healthcare staff from calling for police service as a representative of the organization. In organizations with a full-time security effort, a security representative should make the call for required police service. In organizations without full-time security service, the policy should designate an administrator who will not only approve the call for routine police service, but also generally initiate the call. In times of extreme emergency, the general policy will by necessity be bypassed. The reasoning behind this general policy is basically just good business practice. An organization cannot tolerate employees calling the police for organizational problems without administration or security being aware of the problem and determining whether police service is actually required. For organizations with a security department, the objective is to protect patients, visitors, staff, and facilities whenever possible without assistance from, or intervention by, a law enforcement agency. This objective does not imply that information will be withheld from the police or that necessary police action will not be instituted. It does mean that when the police are called, it must be for a legitimate police problem and not for a management problem that does not warrant police action. Another reason for centralizing the responsibility of calling for police service is to assist the police agency in responding to the proper location. A poor situation is created when, after the police respond to a call, they must spend considerable time tracking down the source of the call to determine where they are needed. A general exception to this policy is cases where the emergency room or other treatment area is reacting to a reportable injury or death of a patient as a matter of business. The administrative policy should not stop at governing calls for police service. The policy should also channel law enforcement officers to report to the security officer or other administrative office when the police have initiated the contact. Obviously, the police are not bound by an administrative policy, but staff contacted by a police officer must determine that proper administrative procedure has been followed by directing the police to the security department. This central reporting assists law enforcement officers in efficiently contacting the proper person to obtain the information

they seek, and it makes the organization aware of the activity taking place. This procedure is also helpful in preventing the disclosure of information to persons fraudulently representing themselves as police officials. Healthcare staff are not always aware that they should require proof of identity before releasing information, or they may in fact accept invalid identification. The policies and procedures just described are intended to benefit both the organization and the law enforcement agency. Because these procedures are mutually beneficial, police agencies should not balk at following these simple, courteous steps. Of course, emergency situations will preclude following a specified procedure in every instance.

## Police Interaction with Patients and Employees

The police frequently need to obtain information from patients. If there are no visiting restrictions for the patient, the police will generally present themselves like any other visitor. When visiting is restricted, the security department may be able to assist the police. Hospitals employ at least two different types of visiting restrictions. The first, for nonmedical reasons, is generally requested by the patient or the family. The second restriction, due to a medical factor, is generally imposed by the attending physician. In either case, security can assist the police by furthering communications with the hospital staff. The request by a law enforcement officer to question a patient must always be referred to the nursing supervisor, who will determine whether the patient is well enough to be interviewed. The nursing supervisor may sometimes need to consult with the attending physician before making this decision. This should not be construed as an indication that the medical care personnel are being uncooperative. It is simply a medical decision that must be made in the best interest of patient care. If medical personnel decide that the patient is too sick to be questioned, the hospital can show its cooperation by notifying the law enforcement agency when the patient's condition improves enough to permit an interview. If the police have a warrant for a patient, the general procedure is to seek medical opinion before allowing the police to serve the warrant, to avoid any medical complications. The police do not always come to medical care facilities to contact patients. Employees may also be the subject of a police interview or arrest. Most police jurisdictions recognize that interviewing people at their place of employment may not always be welcomed by the employer or the employee. In some instances, however, time may be an important factor or the police may not be able to make contact elsewhere. The proper procedure is for the police representative to contact the hospital security representative or Human Resources department, who should produce the employee without delay. The normal protocol is to call employees away from their work area rather than interview them in the presence of coworkers. The facility should also work with the police agency when they have an arrest warrant for an employee. Depending on the seriousness of the charge, the arrest can sometimes be delayed until the work shift has been completed. If an immediate arrest is necessary, employees should be called away from their work area, as in the case of the police interview.

## Emergency Room Activity

The emergency room is usually the scene of considerable police activity. Hospitals are required to report cases of persons seeking treatment concerning gunshot wounds, knifings, rape, etc., as specified by law. This should be the responsibility of the emergency room staff and not the security department. However, the security department should be notified if trouble is expected with a person being treated within the facility. The need for security service may involve patients or persons who have accompanied them to the facility. Hospitals that render a large volume of emergency medical service (EMS), including police-related cases, generally provide accommodations to help the police complete their work, including a room for interviews that is equipped with a telephone. If the security department maintains an office in the emergency treatment area, the police should be permitted to use or share the space. This combination of use not only conserves space but also, if coordinated properly, can promote good relations between the police and the security department.

The security operation is sometimes required to interact with law enforcement agencies, which frequently need to obtain the clothing and personal effects of injured people. If the injured person is under arrest, the police agency is legally entitled to take custody of this property. The hospital should obtain a receipt for all property released. The personal possessions of individuals who are not under arrest may be released only by the patient, an authorized agent, or pursuant to a valid search warrant. If the patient is dead on arrival at the facility and the circumstances of death fall under the legal jurisdiction of the coroner or medical examiner, no property should be released until that office grants authorization. Another area of interaction in the emergency room that may involve the security department is photographing patients for evidential purposes. In these cases, the same basic guidelines prevail as in the release of clothing. The patient who is a police prisoner has little to say in the matter, and the hospital cannot stand between the police and the patient unless a competent medical authority decides that the medical well-being of the patient is at stake. Patients who are not under arrest may be photographed with their approval or, in the case of a minor, with the family's approval. A written photograph consent form should be executed.

Some hospitals in intermediate and large municipalities have problems with law enforcement officers who bring patients to the emergency room and then abruptly leave. Some of these patients create disturbances; others may have no means of transportation home. The hospital ends up with a problem that has little to do with medical treatment. Calls for police assistance with abusive patients who had been "dropped off" by the police are often answered by a different police unit than the one that left the problem on the doorstep. In some cases, police officers must get back in service without delay, but all too often police are simply getting rid of a problem. If a facility experiences this difficulty, it should be handled at the administrative level.

## Detaining Patients

Related to security's involvement with patients and law enforcement is the telephone or radio request from law enforcement to detain a patient. Neither private security officers

nor medical personnel can legally detain patients against their will. The law enforcement agency that requests that a patient be detained should be made aware that patients cannot be legally held. At the same time, stalling tactics are certainly in the best interests of all concerned, particularly if police personnel are en route to the facility. Often if the police do not request that a patient be detained, they may request that security ask the patient to wait for the police. If the patient does leave, information such as type of vehicle, license number, and direction of travel can be obtained to assist the police.

### Prisoners and Police Holds

With the large number of people being cared for today in all types of medical care facilities, it stands to reason that there are many wanted felons among the patient population. Most come and go, and their criminal status is never discovered. There are numerous occasions, however, when a patient is under arrest or serving jail or prison time. The responsibility for ensuring custody of this type of person resides with the criminal justice agency having jurisdiction. Healthcare security officers should not assume any role other than to offer mutually beneficial, noncustody assistance, unless the security department has been contracted to provide specified service. It is becoming quite common for law enforcement and correctional agencies to contract with private security to guard prisoners. Prisoners being treated in TJC-accredited facilities present a standards-compliance issue. There is a requirement that individuals guarding forensic patients be given specific training pertaining to certain healthcare policies, procedures, and protocols. This TJC standard was previously discussed in detail in *Chapter 12, Patient Care Involvement*. An important service that security officers can and should render is to brief the law enforcement representatives about the layout of the area, pointing out escape or intrusion possibilities. The medical facility may also take steps to eliminate or minimize these vulnerabilities. A simple step would be to place the patient in a room that can be secured. If intrusion by others is a concern, locking the doors leading from the stairwell would provide added protection. In brief, security officers should do everything possible to assist the criminal justice agency. Although rare, hospitals have been the scenes of tragic incidents that resulted from forensic patients. It is imperative that hospital admitting personnel and the Emergency Department notify the security department of every forensic patient being treated or admitted. In conjunction with the agency, a decision should be made regarding visiting privileges and the release of information concerning the patient's location.

### Requests for Information

All requests by law enforcement agencies for information about patients being treated should be referred to the security department, or to medical records for information regarding discharged patients. With the introduction of the Health Information Privacy and Accountability Act (HIPPA) of 1996, and Protected Health Information, which is the acts' privacy rule taking effect in 2005, there has been endless confusion and so many

interpretations that the playing field is still less than absolutely clear. What is clear is that billions of dollars have been expended as a result of the act, with tremendous stress on staff and especially patients and families, with little actual gain. One of the problems is that the entities enforcing HIPPA often make up the rules as they go! The facility representative must always make certain that the person requesting the information has been properly identified. If the request for information is made by telephone, extra precautions must be taken. In most cases, information concerning a patient's name, address, birth date, date of admission or discharge, and diagnosis and the name of the attending physician can be released to law enforcement officers. If patient records must be reviewed, or copies released, the law enforcement officer can readily obtain a court order, which will protect the officer and the law enforcement agency, as well as the facility. Because medical and employee personnel records are increasingly being used as a tool for solving legal suits, settling insurance claims, conducting medical research, and other purposes, there are often conflicting opinions on what information can be released. When the guidelines are not absolutely clear, the hospital privacy officer, medical records department, hospital administration, and sometimes, legal counsel, should be involved in the decision.

## Guidelines for Releasing of Information

A set of general guidelines for the release of information to law enforcement agencies by healthcare organizations was developed by the Colorado Hospital Association in cooperation with the Denver District Attorney's office and the Denver Police Department. They are offered as guidelines for all healthcare facilities. It is highly probable that modifications may be required for other jurisdictions, considering all the laws and players involved. For the purposes of these guidelines, the following definitions of medical records were used.

### *Employee Health Record*

This is a record containing the employee's health-related information, such as the employee's physical and medical history. In some healthcare organizations, these records are maintained separately in different locations from other employment information. In other facilities, these records are combined with other employee information and typically stored in the Human Resources department. The distinction is important because information from the personnel record is not privileged and can be released pursuant to criminal investigations, but the employee health record contains privileged communications, and should only be released pursuant to appropriate consents, court order, a search warrant, or grand jury subpoena.

### *Patient Medical Record*

This is a documentation of medical services performed at the direction of a physician or other licensed healthcare provider on behalf of the patient. Patient records do not include notes made by a physician about observations of the patient made while the patient was in a nonhospital setting, which are typically maintained in the physician's office.

*Personnel Record*

This is a record or portion of the record maintained in the Human Resources department, which contains information regarding an employee's basic employment history and performance evaluation. It can be released to law enforcement agencies during criminal investigations without a search warrant or subpoena.

*Privileged Communication*

It is the communication between a physician and an employee or a physician and a patient that is recorded in the employee's health record or in the patient's medical record. Privileged communications occur while the physician is attending the patient or employee and are necessary to enable the physician to prescribe or act for the benefit of the patient or employee. Privileged communications are not generally released without consents and court orders.

*Search Warrants/Grand Jury Subpoena*

A search warrant is a court order issued and signed by a judge. Confidential information and privileged communications must generally be provided pursuant to a search warrant at the time it is presented. Grand jury subpoenas can request that confidential information and privileged communications be presented to the grand jury on a specific date. They are signed by the clerk of the courts.

## Recommended Guidelines Regarding the Release of Information from Personnel Records Pursuant to Criminal Investigation

- All healthcare organizations should designate the individuals to whom requests for information from law enforcement agencies will be referred. The identification of this person(s) should be made known to the appropriate law enforcement agencies, the facility information desk, the admissions department, medical records department, or others deemed appropriate. The individuals designated by the organization should have full authority to provide the information to the requesting law enforcement officer. Law enforcement agencies should make requests for information from the personnel records of the organization during regular business hours. Access to records outside normal business hours is extremely difficult. If it is an emergency, the person in charge of the facility at the request time should have the responsibility and authority to resolve the matter.
- Information should be provided only to a properly identified representative of a law enforcement agency. If the designated individual at the facility who is supplying the information to the law enforcement agency has any doubt as to the validity of the request, the name of the law enforcement officer's supervisor should be obtained, and the agency that employs the officer should be contacted, using the telephone number listed in the telephone book or through directory assistance. When picking

up a record, the law enforcement representative should complete a written request for the information or present copies of court directed action. It should be recognized that the provision of information pursuant to criminal investigations is legal and there is no legal requirement to notify, or not notify, the employee of such information. The provision of the release of information to a law enforcement agency should not expose an organization to any civil liability, if done in good faith. It should be noted that most law enforcement agencies prefer that the employee not be notified of the investigation. It is, therefore, recommended that the organization not notify the employee unless the law enforcement agency indicates that it has no objection.

- If the employee's personnel record also contains employee health or medical information, such as the employee's physical, this information should not be made available to the law enforcement agency without a search warrant or subpoena. If medical information is released by court order, the employee should be given notice of this release of information.
- All healthcare organizations should amend their employment application forms to advise the applicant that while personnel files are not open to the general public, the organization is required to give access to authorized agencies such as law enforcement agencies and other regulatory agencies, including the Boards of Nursing, Boards of Pharmacy, and the Boards of Medical Examiners.

## Recommended Guidelines for the Release of Information from Patient Medical Records

- See Section A of previously discussed Guidelines for Release of Information from Personnel Records.
- The patient's name, address, telephone number, and birth date can be released from patient medical records without requiring a search warrant or grand jury subpoena. Other information may also be appropriate for release. As an example, in a criminal investigation pertaining to drugs, it is possible that information pertaining to the charting of administered medications and the hospital's checkout sheet could be released. The person designated to handle the release of requested information must use his good judgment regarding further release of information, taking into account that law enforcement agencies can get the information by obtaining a court order. The search warrant and grand jury subpoena become public information, subject to public dissemination. It is suggested that an effort be made to work with the local district attorney and law enforcement agency, to voluntarily provide appropriate information and minimize the necessity of obtaining search warrants and grand jury subpoenas. Law enforcement agencies should recognize that the point at which a healthcare organization will require a search warrant or grand jury subpoena for further release of information may vary slightly from facility to facility.



## When Providing Information from Personnel, Employee Health or Medical Records Pursuant to Search Warrants or Grand Jury Subpoenas

- Legible copies of the requested record should be provided and should be acceptable to the law enforcement agency. The original can be made available for comparison purposes, but should not be removed from the hospital premises unless in the custody of a hospital employee.
- Determine that the search warrant or subpoena is authentic. All search warrants must be signed by a judge. Grand jury subpoenas for criminal investigations will be signed by the clerk of the court.
- Carefully review the warrant or subpoena to determine the specific information requested and supply only that information. Record the name of the individual who was supplied with the information and maintain a copy of the warrant or subpoena.
- If privileged communication is being sought by a law enforcement agency pursuant to a search warrant, it must be provided when requested and the individual notified thereafter. When privileged communication is requested pursuant to a subpoena, there will be time to notify the individual before the communication is made available to the grand jury. Notification will allow the individual an opportunity to take appropriate steps to protect the privileged communication.

## Key Considerations for Information Release

- The law enforcement agency must obtain its evidence in a legal manner or it will not be admissible in court, so they must follow certain guidelines.
- It is desirable, and in the best interest of all concerned, including those under investigation, to ensure fairness and to protect the integrity of the investigation, to keep the information within the investigating agency.
- If the information requested by law enforcement agencies can be supplied voluntarily within the law by hospitals, it will be unnecessary for the law enforcement agencies to obtain search warrants or subpoenas. It should be noted that once a search warrant is filed for or a subpoena requested, the case becomes public information.
- If there is disagreement between the law enforcement agency and the hospital as to the information to be released, it is recommended that the hospital contact the local district attorney's office that is involved and attempt to resolve the problem.
- It should be understood by law enforcement agencies that there may be some instances in which the hospital would prefer that a search warrant or subpoena be obtained prior to release of the information. This request should not be viewed by law enforcement as the hospital being uncooperative.
- Police investigation files are confidential; therefore, release of information to a law enforcement agency is not a release to the public. Also, if the information is information to which the law enforcement agency can compel access through the

courts, there would seem to be no basis for liability against the hospital just because it made the information available voluntarily.

## Security and Law Enforcement Liaison

The discussion thus far has revolved around the security department's operational relationship with law enforcement. In addition, security administrators must foster good formal and informal everyday law enforcement relationships. The most common method is direct, goodwill contact with agency personnel. In addition, one of the best methods of fostering law enforcement liaison is to show various agencies that the security program is a professional program that supports the law enforcement mission at every opportunity. One example of this support is that of enhancing public responder safety. Private security is increasingly forming a vital link between the citizen and emergency service providers. As part of this link, security officers are often the ones to report emergency situations or crimes in progress. The information they report and their support at the scene can be very instrumental in providing an extra measure of safety to the responder. Another example of showing organizational support for the police is to provide a room that the police can access to talk with a person of interest, including victims. This room is usually located in the emergency department and may be equipped with communications equipment, computers, beverages, and snacks. Officers are encouraged to complete their reports in this out-of-the-way area while still being available as a presence in the facility. It is not uncommon to include signage that the room is for police and other public safety personnel, such as fire and EMS staff. It is also not uncommon to share the room as a combination of public safety and security officer/work area.

## Community Programs

Various local programs also work toward security/law enforcement cooperative efforts. Cities throughout the United States and Canada have created, usually through legislation, special business improvement districts (BIDs) to increase safety and to keep streets clean. In 1994, there were over 1,000 such districts in the United States and Canada, including 24 districts in New York City alone. One of the best-known and most highly regarded districts is the Central Philadelphia Development Corporation. It was first created in 1991 for a period of five years. The public, police, and private security program was so successful in reducing crime and improving safety that the City Council extended the program for 20 years in 1995. There are approximately 50 security officers who are officially known as Community Service Representatives, providing security patrols alongside the regular police officers assigned. The security force has offices in the police substation serving the district.<sup>7</sup>

## Frequency of Law Enforcement Contacts

Security can become a nuisance in constantly promoting and contacting the police for both liaison and called-for service. The professional healthcare security administrator

**Table 13-1** Frequency of Security Directors' Contact with Law Enforcement Agencies

Daily	10.6%
Weekly	33.3%
Twice a month	25.8%
Monthly	15.2%
Less than once a month	10.6%
Never	3.0%
No answer	1.5%

will not force unimportant contacts with the police. The message that the police need to understand, and believe in, is that when the police are contacted, it is because the police are truly needed or that security has significant information to pass on.

A survey of Security Directors/Safety/Loss Prevention<sup>8</sup> persons asked how often they interacted with the local Police Department. The results are listed in [Table 13-1](#).

It is not always security administrators who initiate or foster a good relationship with law enforcement. Progressive law enforcement agencies often take the lead in this endeavor. It is projected that police and security operations will work together to a greater extent in the future. On the basis of study research, William Tafoya of the FBI Academy predicts that by the year 2035, half of all law enforcement duties will be assumed by private security companies. In 1990, it was estimated that police officers spend 80% of their time performing services rather than traditional law enforcement duties. In many communities, police and security are already sharing training programs and information, and private industry is training police officers in such areas as computer systems and corporate security.<sup>9</sup>

### Potential Adverse Relations with Police

Security programs that utilize off-duty police officers, in full or in part, to staff security positions should be aware of a potential conflict that can arise. This conflict can occur when the services of a specific police officer are no longer needed by the healthcare organization and the officer is terminated for cause. These terminations are not always amicable and hard feelings on the part of the police officer may have an overall negative impact on the healthcare organization. A police officer imparting displeasure with the healthcare organization can result in damaging the relationship between the two entities, curtailment of certain police services, and slowdown in response time for calls for service, among other things. The security administrator needs to evaluate what steps can be taken before and after such an event to mitigate the negative impact on the organization.

### Security and Nonpolice Liaison

The fire department is a public safety agency that has frequent contact with healthcare organizations as a whole, and specifically with hospitals. These contacts take the form of

fire prevention and inspections and emergency response. In most cases, the interaction of the organization with the fire department is more in the arena of safety as opposed to security. Security does, however, play an important role in emergency fire response. This role pertains to providing efficient access to the facility and guiding the first responders to the alarm locations. Proper actions by security personnel can save valuable time, which is critical in fire situations. Although infrequent contact may be made with the office of emergency preparedness on local, state, or federal levels, the security department is vital to their planning efforts.

## References

1. National Advisory Committee on Criminal Justice Standards and Goals. (1976). *Private security: Report of the task force on private security*. Washington, DC: Van Meter, C p. 4.
2. Gunter, W., & Kidwell, J. (2004). *Law enforcement and private security liaison: Partnerships for cooperation*. Available at <http://www.ifpo.org/articlebank/lawprivateliason.html>. Retrieved on June 24, 2009.
3. Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to security* (8th ed.). Burlington, MA: Butterworth-Heinemann pp. 60–61.
4. White, B. (2009, April 21). Cash-strapped cities try private guards over police. *Wall Street Journal*. Available at <http://online.wsj.com/article/SB124027127337237011.html>. Retrieved on June 24, 2009.
5. Farber, O. (2006). Positive SPIN on liaisons. *Security Management* (June), 110–120.
6. Blades, M. (2008). Helping hands. *Security Technology & Design* (May), 36.
7. Seamon, T. M. (1995). Private forces for public good. *Security Management* (September), 92–93.
8. Radford, J. (2001, May). Public private partnership. *Access control & security systems*. Available at [http://securitysolutions.com/mag/security\\_publicprivate\\_partnerships/index.html](http://securitysolutions.com/mag/security_publicprivate_partnerships/index.html). Retrieved on June 24, 2009.
9. Future of security-shared resources. (1988). *Security Magazine* (June), 16.

# Human Resources and Staff Responsibilities

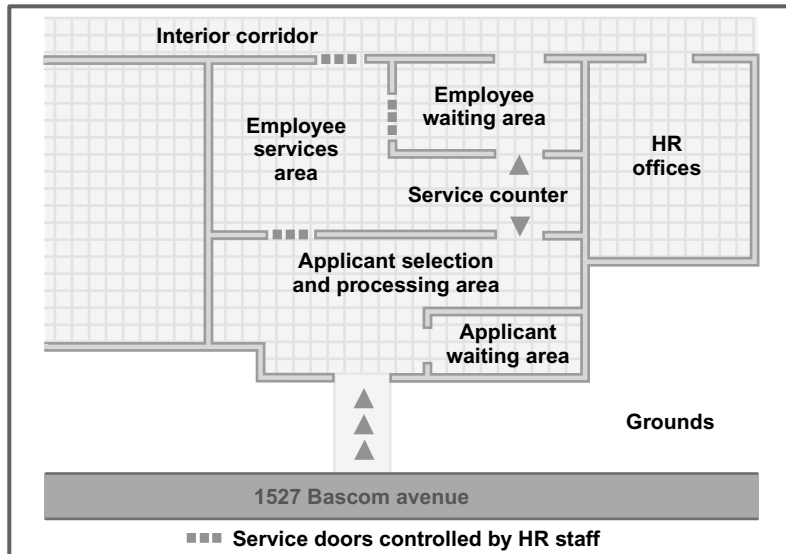
The protection system in medical care facilities interfaces directly with the human resources (HR) department. The security program is charged with enforcing rules and regulations, which in many cases were promulgated by the HR department. Furthermore, security incidents often involve employees, and the HR department along with a supervisor of the employee's department may be involved in determining what action, if any, is to be taken against the employee. Also of extreme importance to the security function is immediate access to personnel records for investigative purposes. Conversely, in doing their job, HR personnel are often dependent on security department records and expertise in obtaining pertinent data for a variety of situations from sources inside and outside the organization.

The security and HR departments, like all other departments in the organization, must support one another in providing a system of protection that is beneficial to the entire organization. This mutual support does not occur without the effort of both the parties. There is an inherent conflict between the general goals and objectives of HR and those of Security. HR has a basic mission of being an advocate for the employee, which at times may overshadow the basic mission of the organization. Security, on the other hand, has the responsibility to provide a reasonably safe environment for all persons and to protect the nonhuman assets of the organization. Security must understand the legal rights and display proper employee respect. HR must understand that wrongdoing, or suspected wrongdoing, of an employee cannot go unresolved in the interest of sustaining excellence in patient care through a respected, successful, and sustainable healthcare organization. A heavy-handed security approach or an overly burdensome bureaucratic approach by HR does not serve the organization in the appropriate manner. Leadership of HR and Security should work together, as partners, in providing the best level of patient care possible.

There are various HR activities and functions that bear directly, or indirectly, on the security posture of the organization. Included in this area are access control of applicants, staff identification systems, background investigations, disciplinary actions, assisting in investigative activity, and fostering proper employee conduct.

## Human Resources Office

The location of the HR office is an important security consideration. The objective should be to keep applicants out of the main facility. Not only may applicants interfere



**FIGURE 14-1** Example of a human resources department with an outside entrance for applicants and an internal entrance for serving employees.

with clinical care, but they also have been known to commit various security infractions while “looking for a job.” Further, applicants—who may also be potential malefactors—should not be given the opportunity to become unduly familiar with the facility’s layout and design. The employment (applicant intake and screening) portion of the HR department should either be in a separate building or have its own entry and an individual street address to discourage access to the main facility. [Figure 14-1](#) shows a layout for an HR department that has a street entry point for applicants and a separate internal entry point for serving employees.

Some healthcare organizations have moved the applicant screening and processing function off campus. The offsite screening of applicants has very positive security benefits. Also, organizations that utilize state or local employment commissions to screen positions that draw a large number of applicants have reported great success with this third-party approach to the hiring process. From the security point of view, it does the same thing as an organization offsite model in that it reduces the amount of applicant traffic accessing the main treatment facility.

## Selecting Staff Through Due Diligence

Healthcare organizations must search out new and better ways to effectively reduce the incidence of employee misconduct and the commission of crimes against the organization and its stakeholders. The best place to begin this effort is to exercise due diligence in the selection of new staff. It is generally accepted that employees who have a history of bad or undesirable conduct are likely to continue this behavior into the future.

We are all familiar with the multitude of problems associated with poor hiring practices. A recent media headline read, “Supervisor Blamed for Rapist Hire at Hospital.” In this case, top Los Angeles County health officials tried in vain to explain how an ex-police officer convicted of rape was hired not once but twice to work in public hospitals in a position of providing care. The county hiring process failed to perform a “live-scan” background check for convictions.<sup>1</sup>

The best security investment an organization can make is to expend the necessary funds to properly screen job applicants. It is generally accepted by personnel and security experts that 20% of any given workforce is responsible for 80% of various personnel problems. There is further agreement that an estimated 90% of all persons known to have stolen from their employers were not prosecuted.<sup>2</sup> Not only should job applicants be properly screened, but current employees being considered for promotion to an area where there may be significant security risks should also be rescreened. A general rule for rescreening for promotional reasons is if it has been over 5 years since the employee was screened as an applicant. Prescreening may also be for a particular investigative purpose. There are screening firms that offer database repositories that allow enrollment of an employee in a service that will alert the employer if an employee has a record entered into the database at any time in the future. This service is a way to implement an ongoing employee screening program, giving a visibility beyond the preemployment background check.<sup>3</sup>

The employee selection process is an area in which the healthcare industry as a whole receives poor marks. In too many cases, HR departments have simply been deficient in properly screening applicants. The healthcare industry, like most industries, attracts applicants who are not always honest and often neglect to reveal items that would prohibit their hiring. There are thousands of cases demonstrating why proper screening is so important. The healthcare industry is filled with stories of applicants for nursing positions who neglect to identify convictions for fraud, drug theft, or physical abuse against the elderly to the registered sex offender seeking employment as a phlebotomist.

It has become increasingly difficult to seek information relative to hiring appropriate staff with the restrictions imposed by legislature and court-imposed constraints. The problem is further exacerbated, on the other hand, by the courts for holding employers liable for negligent hiring. The current state of these limiting controls and sanctions is directly responsible for much of our workplace violence and the billions of dollars lost to employee defalcations. These dollars must be paid either directly, or indirectly, by all of society. Despite these constraints, there are methods and procedures to deny employment to dishonest and dangerous applicants. The HR department must therefore provide a high level of due diligence in the employee selection process.

## Applicant Suitability Information

There will always be some flawed hiring decisions; however, the number of bad decisions will decrease when more in-depth information regarding the applicant is sought

and properly evaluated. Information relative to an applicant's suitability for employment can be developed through various methods, including a properly constructed and completed application form; various databases, contacts with previous employers; verification of information through official public records, a variety of tests; and information from friends and previous co-workers. A policy and process of due diligence hiring send a clear and powerful message that it is the intention of the healthcare organization to protect patients, staff, and visitors.

## Employment Application Forms

A good employee selection process begins with the proper design of the application form. The form must be designed with security in mind along with the primary business objectives of the organization. All applications must ask whether the applicant has been convicted of any crime (misdemeanors and felonies, excluding traffic offenses). Although there is some use of online application processes that allow applicants to input their own data, the applicant should at some point be required to fill out an application on site. There is much to be learned about an individual from the manner (completeness, spelling, neatness, etc.) in which the application is completed and submitted. It is important to know that the applicant has indeed completed the application rather than a friend or relative. Employees should be required to formally update application information annually, including criminal convictions. This can be accomplished as part of the formal employee evaluation process.

Although every applicant accepted for employment is required to comply with the policies, rules, and regulations of the organization, many organizations have found it helpful to use conditions of employment or employment agreements. These conditions are usually attached to the application form, although in some instances the conditions are incorporated into the application itself.

## Applicant Background Verification

Nowhere is background screening more important than institutions that directly impact the public, such as hospitals. Recruiters, security professionals, and top management continue to agree that much more must be done in the area of applicant background, verification, and investigation to properly protect patients, staff, and property. The courts generally support this view. The problem that presents itself is that the courts render judgments for inadequate hiring processes, yet in other decisions they make it virtually impossible for organizations to obtain any significant background information. It is the opinion of many security and police administrators that the Federal Privacy Act has done great harm to employers and has, in fact, encouraged greater criminal activity. Many believe that the rights of employers, and society in general, have been negated to the point that effective applicant screening is often more of a myth than a reality. As a result,



many protection systems are geared to reacting to problems involving employees rather than preventing such situations through good hiring practices. Courts and most government agencies set up to protect employees' rights have indicated insensitivity to the cost of crime and the suffering of victims. Despite this insensitivity, medical care facilities must continue to do everything possible to employ individuals who contribute to excellence in patient care and protect the assets of the organization. There are a myriad of federal and state laws that restrict the use of certain applicant information in the hiring process. The two basic federal laws of most significance that affect the hiring or demotion process are the Equal Employment Opportunity Commission (EEOC) and the Fair Credit Reporting Act (FCRA).

## Deceptive Applicant Information

Applicants are not always truthful in the information provided on their application form. The top five “lies” told by job applicants, according to a large screening provider, are:

- Exaggerating dates of past employment. As many as 34% of resumes and application information include discrepancies related to previous employment. The most common reason is to cover gaps in their work history they may not want to explain or to be known.
- Falsifying the degree or credential earned. As many as 20% of applicants falsify their education or credential achievements.
- Inflating salaries or title. It seems the motive is to appear more qualified to fit a requirement or qualify for a better job or higher salary.
- Concealing a criminal record. There is an approximate 11% of applicants that claim no criminal record when in fact they have such a record.
- Hiding a drug habit. Since 42% of Americans admit to using illegal drugs in their lifetime, it stands to reason that this is an important area of screening, especially for healthcare organizations.<sup>4</sup>

## Background Screening Providers

The vast majority of healthcare organizations use varying levels of service of third-party background screening companies. There are hundreds of these providers with a vast array of service offerings. The service offerings of background checking available include such items as employment verifications, criminal histories, education, credentialing, references, credit reports, motor vehicle reports, and date of birth statements, to name some of the most common. When using a background screening company, the healthcare organization generally selects a basic package of background elements to be checked for all applicants. They then have the option of adding elements for selected positions. For example, education, credentialing, and credit reports may be prudent for certain positions but not necessary for others.

Not all background checking services are equal. Just as applicant information must be checked and verified, so should the third-party provider of background checking be vetted. It is incumbent on the healthcare organization to investigate the third-party provider of background information relative to accuracy of information provided and the timeliness of receiving the information requested. Applying screening arbitrarily and without a carefully formulated plan can leave patients, staff, and visitors vulnerable and the healthcare institution liable for criticism or litigation. It is important to make background screening a consistent and automatic part of the hiring process and healthcare protection program without falling into a “check the box” routine. The National Association of Professional Background Screeners (NAPBS) is an association that may be helpful in providing information when an organization is developing its hiring practices.

A criminology professor at the University of Maryland recently decided to check on the services of an online database service provider. The professor obtained the records of 120 parolees in Virginia and submitted their names to the database company for a criminal history record check. The return information reported 60 names with no criminal record and additional names that the information was so difficult to interpret that it was extremely difficult to determine the nature of the offenses.<sup>5</sup>

## The Extended Workforce Loophole

There is the presence of a largely unscreened extended workforce performing everyday services in our nation’s healthcare facilities (HCFs). Even where there is a stringent employee screening process, there is often no plan, program, or process for vetting vendors, contract staff, temporary workers, volunteers, and others performing ongoing services that are not employees of the healthcare organization. This vulnerability is highlighted by a recent survey of vendor/contract employees that concluded that this extended workforce staff was 92% more likely to have a felony record than an organizational hire and 50% more likely to have a misdemeanor record or drug history. One explanation of this striking difference is the theory of “adverse selection.” Since so many healthcare organizations conduct solid background checks as part of their standard hiring process, applicants with questionable pasts tend to find jobs with companies where background checks are not performed or not performed in an adequate manner. The message is clear that healthcare organizations must develop specific background screening requirements (standards) for all companies rendering contract services on campus. With the average court award for litigation involving negligent hiring and retention of employees exceeding \$1 million, there is significant liability for the healthcare organization, even if the indirect employee is hired and paid by another organization.<sup>6</sup>

## Security Role in the Hiring Process

An increasing number of medical care organizations rely on their security departments to assist in screening applicants. In some cases, only applicants for the so-called sensitive

positions are subject to security input, but in other organizations, all applicants are the subjects, to varying degrees, of security background investigations. Since unfit employees tend to move from one medical care facility to another, new and improved methods of facility interaction must be put into place to prevent these employees from repeatedly victimizing healthcare organizations. The advent of large healthcare systems provides an opportunity to at least consolidate employee information within the system.

## Staff Identification Badges

Healthcare organizations must provide each employee with identification. It is a common practice to provide this identification, utilizing a picture badge to be worn by all staff. The rapid increase in the use of electronic card access systems in HCFs has resulted in one badge that has multiple uses. The identification badge utilized in healthcare provider organizations has several basic purposes. One purpose is to function as a basic element of the access control system and to accomplish an electronic time-keeping function. Second, it serves the purpose of compliance with TJC standard, which requires that all patients have the right to know who is the person providing direct patient clinical care. The IAHSS has developed the following basic security guideline relative to staff identification.

### IAHSS—HEALTHCARE BASIC GUIDELINE, #07.01

#### **Access-Control Identification System**

**STATEMENT:** Healthcare facilities (HCFs) will maintain an identification system that identifies all general staff, “General Staff” being defined as all personnel regularly serving the HCF: e.g., employees, volunteers, physicians, students, and regularly scheduled contract service staff.

#### **INTENT:**

- a. A color photographic likeness, unique identifiers, and an expiration date should be incorporated onto the HCF's identification badge.
- b. Information contained on ID badges (i.e., credentialing, job title, department) should be verified at employment and at the time of reissue.
- c. Identification badges should be worn and properly displayed at all times while on the property owned or controlled by the HCF, except when the person is a patient presenting for medical care or when visiting a patient.
- d. The HCF should maintain a “current personnel policy” with aggressive deactivation of identification badges along with a system for the collection of badges upon separation from the HCF.
- e. The HCF should expire and reissue previously issued badges at a minimum of five (5) years from the date of issue.
- f. The HCF should have a policy that pertains to the identification of outside vendors (e.g., sales persons, repair persons, service persons, contractors) providing services within the HCF.

- g. Regularly scheduled contract personnel are those persons who are employed by an outside company which is contracted by the HCF to perform departmental functions such as contracted food service, environmental services, security, biomedical engineering, etc.
- h. In some cases, by formal policy, the HCF may accept identification badges issued by another organization, e.g., student badges issued by another university, college, or other HCF.
- i. Consider utilization of the HCF ID badge as a credential authenticating emergency response workers.

**Approved:** January 2006

**Last Revised:** October 2008

## Administering the Identification Badge Program

There are several key security issues relative to the administration of staff identification systems. First, the system must provide for expeditious replacement of lost or stolen cards or badges. However, replacement procedures often make it easy for staff to obtain two badges, if they desire, by claiming they have lost their badge. They can then turn in one badge at termination and still retain the second badge for various purposes. Even organizations that make a substantial effort to control employee identification badges can easily fail to retrieve as much as 20–30% of the badges issued. Fortunately, in most cases, the uncollected badges are not used for negative purposes. A major advantage of the electronic card access identification system is that a badge can be immediately deactivated. Not all badges are recovered and one east coast hospital found that its policy to immediately deactivate its hospital-issued badges prevented a former employee from accessing the secured birth center and carrying out a plan to abduct an infant from the facility.

Funding is always an issue. All identification badge systems cost money, and while the cost of the materials needed to produce the cards is a rather small percentage of the total program cost, in projecting material costs, there is a tendency to underestimate the number of badges that will be produced. The number of badges an organization will require annually is generally at least two-and-a-half times the number of actual authorized positions. This estimate allows for lost cards, name changes, position changes, cards ruined in the production process, and staff turnover. One organization reports that it used 2,850 cards the first year for an average of 880 employees during the year.

Although the front of the badge normally contains only the picture, expiration date, name, and departmental or position information, the reverse side of the badge is often used for other pertinent information. The reverse side of the badge can be used to display the security telephone number, code information, or even a brief description of emergency procedures. Since space on the badge is limited, it is not uncommon to find a second laminated information card attached to the primary badge. Recently, the TJC surveyors

have not looked with favor on these cards containing emergency response information. A growing trend is to provide badges that are identical on the front and the back. In this respect, the badge is a two-sided badge without a front and back. The two-sided badge generally solves the problem of the employee inadvertently, or intentionally, turning the badge over (inward), hiding the identity of the person.

The most common problem in any employee badge identification system is obtaining compliance of displaying (wearing) the badge as prescribed. A certain number of employees will always resist, and organizations that initiate a badging program must be prepared to provide strong administrative support. Organizations can take actions to promote voluntary compliance. Chief among these actions is to make the badge useful to staff. In other words, the more often the staff have their badges to engage in certain activities during their shift, the more apt they are to wear them. Also of paramount importance in promoting compliance with the program is for top administrative personnel to set a good example by always displaying their badges. In one program, the badge system was initiated by issuing badges to supervisory personnel 2 weeks before they were distributed to the other staff members. Not only did this procedure set a good example, but it also generated interest among staff, who wanted to know when they were going to get their badges. In another program, the badge had a designated place to affix employee longevity award logos. When employees reach their fifth year of service, for example, they are issued a new employee badge with the award logo. This system provides a practical means of recognition; other award pins often end up at home in a dresser drawer. In some programs, so many stickers and other items are attached to badges that the whole purpose of identification badging is defeated. A strict policy should be in place to address this issue. The problem of “badge clutter” has been solved to some extent with the extensive use of electronic access control systems activated by Radio Frequency (RF) technology. These badges contain internal wires that, if punctured, will render the badge useless, and thus pins of any kind cannot be affixed to the badge.

## Identification Badge Design Considerations

The name of the individual must be of sufficient size so that it can be read from a distance of at least 2 or 3 feet. An 18-point type allows the name and position to be read from a distance of approximately 8–10 feet. It is important that the organization be able to produce the badge in-house so that it is ready for an employee’s first day on the job. This capability is also important in preparing a new badge in the event of a loss or name or status change. When badges can be quickly produced by the organization, employees will not be without a badge, and the entire process can be completed in only one trip to the processing station. The use of specific job titles on the badge will necessitate considerably more changes than the use of a more general title or department designation. For example, it would be better to include “Food Services” on all badges issued to that department, rather than “Head Cook,” “Dishwasher,” “Tray Attendant,” etc. In clinical

areas, more precise titles, positions, and/or credentials are required to more properly identify the employee for purposes of patient treatment and interactions.

A system of issuing temporary badges must be established. Employees should not be allowed to work without a badge if it was left at home or misplaced; they should receive a temporary badge. In some systems, the temporary badge must be checked in when employees have completed their shift. In other systems, the temporary badge is issued for a given shift or a specific number of days. Employees should be given a choice of a pin clip or other means of affixing the badge. Some organizations allow the badge to be affixed to a chain worn around the neck. Giving employees this choice is intended to enhance compliance with wearing the badge. In some badging programs, contractors, salespeople, students, and others who perform a service within the facility are badged as well as employees. These badges can be permanent issue or, in the case of a contractor or salesperson, can be issued for set number of days.

Using color codes to denote the various authorized areas that the bearer may enter does not usually work well within medical care facilities. All employees should be issued the same type and color of badge, except for staff assigned to a mother/infant unit. Different types or colors may be helpful for temporary badges to identify contractors, salespeople, clergy, and others.

Physicians should be required to wear identification badges, just as other staff. In order to promote wearing the badges, there must be strong medical director support. As a general rule, physicians have historically resisted badging. House staff (interns and residents), which usually receive training by rotating among several facilities, are often able to utilize a single medical school or teaching hospital identification badge in multiple facilities. In these cases, all participating facilities must be party to a structured, formal agreement regarding this type of arrangement. Since the staff of any specific organization is responsible to challenge other caregivers who are not properly identified, there must be a communication link in regard to *accepted* identification from other organizations.

## Security-Oriented Employment Guidelines

A major function of the protection system is to manage employee actions and conduct while protecting the organization's well-being by enforcing organizational rules and regulations. Concise, written personnel policies provide a solid foundation on which to regulate staff conduct. Vague, unwritten policies benefit neither the staff nor the organization. Commonly, employment guidelines are contained in an employee handbook or administrative policy. Although policies for sick leave, vacation time, wages and hours, disciplinary action, etc. are always carefully spelled out, security policies are often ambiguous or omitted entirely. Policies affecting staff must be tailored to the type of facility and to what is expected of staff in that facility. However, certain basic security policies are germane to every medical care facility. Some of the most important security policies are discussed here.

## Employee Security Responsibility

A unique aspect of healthcare security is the important role every staff member plays in providing an adequate level of protection for the facility. It is important that every organization clearly set forth the employee's responsibility for security. A typical policy, which should be part of every healthcare organization's policy, is as follows:

*It is the responsibility of every employee to be aware of anything observed that may affect the welfare of the patients, other people on the premises, or the physical property of either individuals or the organization. When any such observation is made, employees will take steps to investigate further, intervene if time is of the essence, and report the circumstances to their supervisor and the security department. Further, it is the responsibility of every employee to report any and all threats to staff, visitors, or patients in accordance with the facility threat policy.*

## Off-Duty Employees

Many facilities face serious problems with off-duty employees who remain in the facility after their shift ends or who return to the facility on their off time to visit other employees. These visits not only waste the time of employees on duty, but can also result in other problems, such as disturbances, loud and noisy activity, drinking, drug use, and property losses. The following is a typical policy pertaining to this problem:

*Employees who are not on duty should not be on medical center property more than 30 minutes after their work shift or more than 30 minutes before the start of a scheduled work shift. Employees who are off duty may return to the facility to receive medical care or to visit a patient, or they may return with the specific authorization of an administrator or supervisor for a specific purpose, such as a staff meeting, training activity, or volunteer type of service.*

## Employee Weapons

Unfortunately, many healthcare employees carry weapons to their place of employment. Whatever the purpose, the possession of weapons on facility property should be prohibited. Because almost anything can be construed as a weapon, the policy established should define which weapons are specifically prohibited. The following is an example of a weapons policy:

*Employees are prohibited from bringing weapons or explosives onto hospital property. For the purpose of this policy, weapon is defined as any gun, loaded or unloaded, any knife with a blade longer than three inches, or any weapon that by law is illegal to possess.*

It is noted that currently there is considerable pending legislation in a number of US states that allows employees to have a gun, loaded or unloaded, in their parked vehicle while at work.

## Package Inspection

The control of packages and equipment entering or leaving the facility is a major security management issue. The primary concern is for egress; however, at times, ingress is also an issue relative to contraband entering the facility. Effective control requires the compliance and cooperation of all staff, as well as the control of various facility entrances and exits. Unfortunately, most healthcare security programs are not adequately staffed to enable them to control all egress points. As a result, package inspection is conducted as a spot-check or is incidental to patrol services. A good access control program depends largely on the ability to designate and enforce a policy that authorizes only certain doors for staff use. The property pass is widely used, but only yields varying degrees of success. Although they differ considerably from facility to facility, pass programs have the common objective of discouraging theft and providing property accountability. These systems establish a sound basis for security officers to inquire about employees observed carrying an item from the facility. In some programs only organization property is subject to the pass policy, which creates the problem of determining what is personal and what is organization property. A package inspection policy should cover not only packages being taken from the facility, but also those being brought in. The following is a typical policy:

*All property being taken from or brought into medical center buildings or upon medical center property is subject to inspection by security officers or medical center administrative personnel. Any medical center property, regardless of value, being taken from the property shall be accompanied by dated, written authorization form that contains a description of the property and the name of the person authorizing removal.*

All property pass systems should be well organized to eliminate as many weaknesses as possible. If reasonable compliance appears doubtful, it might be better not to implement the pass system at all. One commonly cited weakness in property pass programs is the lack of feedback to department management. In too many programs, passes are simply collected and discarded. Collected passes, or a copy of such passes, should be returned to the authorizing department for review and audit purposes. [Figure 14-2](#) is an example of a property removal pass.

Of course, an organization can maintain a property inspection system without a formalized property pass. In other words, security personnel may still inspect property to determine whether its removal has been authorized. The following policy statements are offered as a sample of an inspection system policy/procedure.



UNITED MEMORIAL HOSPITAL PROPERTY REMOVAL AUTHORIZATION	
Date: _____	Time: _____
Name: _____ Staff ___ Visitor ___ Patient ___	
<b>Has permission to remove the following property from the UMH campus (Describe fully: amount, color, type of property):</b>	
Property: Surplus ___ Obsolete ___ Loan ___	
Other (explain): _____	
Authorization Signature: _____	Position: _____
Department/Service: _____	Tel. Ext. _____
<b>Prepare in Duplicate – Forward Copy to Security Services</b>	

**FIGURE 14-2** Example of a property removal pass.

#### *Cause to Believe That Contraband or Stolen Property Is Being Transported*

On occasion the security officer will receive information that a possible theft will occur; receive a request for an inspection of a person or persons by a facility administrator or supervisor; or observe extremely suspicious activity. In the case of the first two circumstances, the officer should confer with a security supervisor if time and extent of the problem permit. In the case of activity in progress, good officer judgment will prevail.

#### *Observation of Exposed Equipment*

Often, an item of possible medical center property is observed being removed from a facility and does not fall under the suspicious activity category. Open-view removal generally indicates legitimate removal; however, the security officer should make tactful inquiry as to ownership. The legitimate person will seldom take offense, and the procedure helps to solidify the image that the facility is concerned about the safety and protection of its environment.

*Concentrated Package Inspection*

Such package inspection is a planned security operation under the supervision of a security supervisor per direction of the Security Director. Security personnel will be assigned to a specific exit and check property being removed by any person. In this regard, purses and lunch boxes will be excluded unless the purse is extremely large.

*Identified Medical Center Property*

The person removing the property should be identified. If the person is a medical center employee, the person should be allowed to proceed after a list of the property has been prepared and the employee's department verified. The department will be called to verify authorized removal if the officer deems such action necessary. If the person removing the property is not an employee, the employee authorizing removal should be contacted.

*Suspected Medical Center Property*

The security officer should prepare a list of the property and identify the person, who may then proceed on his way. Complete documentation of package inspection is of course mandatory. Also, employees should be reminded periodically of the policy concerning property inspection. Two methods are the hospital newsletter and handbill-style notices. During a concentrated package inspection, security officers may hand these notices to employees who are surprised by or express ignorance of the policy.

## Cooperating with an Investigation

Investigations of all kinds are a continuous process in most healthcare organizations. Although the concern here is for security-related investigations, healthcare organizations conduct other investigations to collect and analyze facts for various business and patient-care situations. To efficiently and thoroughly carry out this investigative activity, employers must have the full cooperation of all staff. A policy such as the one that follows should be strongly considered for any healthcare organization:

*All employees are required to cooperate fully with any medical center supervisor, manager, or member of the security department who is conducting an investigation or inquiry on behalf of the medical center. Failure to provide cooperation may be considered as insubordination and may subject the employee to disciplinary action.*

## Staff Lockers

A frequent concern for healthcare organizations is the staff locker. Lockers furnished to employees for use in connection with their employment should be inspected periodically. Two supervisory staff members, one from security and one from a relevant department, should conduct the inspection. To maintain proper control of staff lockers, personal locks should not be permitted. If the facility does not furnish locks, staff must provide their

own. In this situation, the organization must still retain access to the lockers. Staff should be required to furnish a duplicate key or the lock combination to the department responsible for the staff locker program. The following is a typical policy for staff:

*Staff lockers are the property of the medical center and are subject to inspection at any time for sanitary or administrative purposes. No medical center property will be stored in an employee locker, except such property issued to the employee for which he or she is personally responsible.*

### Staff Solicitation and Distribution of Products

Virtually all HCFs have a policy on solicitation, which generally pertains to both employees and individuals from outside the organization. However, many organizations do not include in this solicitation policy the free distribution of products or materials. In one sense, this distribution could be viewed as indirect solicitation, but not always. One hospital reports that an author of a paperback book came to the hospital and began visiting patients at random, leaving them a complimentary copy of his book for their reading pleasure. The hospital did not know anything of this situation until one patient complained that the book was pornographic. After a review of the book, the hospital visited patient rooms with an apology and hastily retrieved the books. The author was contacted and he stated that his purpose was to simply provide reading material to help cheer up the patients. He was asked to immediately cease and desist his activity. Medical care organizations cannot carry out their work efficiently while permitting solicitation or the distribution of materials to staff or patients. The following is an example of a solicitation and distribution policy:

*To protect employees and patients from annoyance or disruption, no solicitation or distribution of products or materials of any kind by employees or outside persons is permitted on medical center property without the express permission of the medical center administration. This prohibition includes circulating petitions, selling merchandise, selling chances for a lottery or drawing, or distributing products or literature. All staff members have an obligation to report any such solicitation or distribution of products to their immediate supervisor.*

### Gifts from Patients or Family

Staff should be prohibited from accepting gifts or gratuities from patients or their families. Employees are paid to provide their services, and the acceptance of any form of gift fosters possible abuse such as favoritism, special treatment, and fraudulent practices. The enforcement of this policy rests with departmental supervisors and rarely becomes a security issue. There may be some exceptions authorized by administration, such as with valet parking, but these exceptions should be well thought out and limited to only a small number of such exceptions.

## Employee Time Recording

The concern for the loss of tangible hospital assets often overshadows the loss of employee time. However, organizations lose money every day by paying for time that employees do not work. Although the improper recording of time is a supervisory problem, the security department may become involved in an investigation of fraudulent time recording activities. All organizations should maintain a policy that strictly prohibits an employee from recording time for another employee. An example of such a policy is:

*No employee will record time on a time card belonging to another employee or through electronic means. No employee will allow another person to record time on their behalf.*

The problem of fraudulent recording increases as organizations grow in size. The larger and more impersonal an organization becomes, the better the climate for the theft of time. Virtually every department and section of the organization is vulnerable to this often-ignored source of financial loss. The concept of flexible work schedules (flex time) renders the control of time records and the surveillance of employee traffic more difficult. Within certain defined parameters, flex time programs allow employees to report for work on their own schedule, after which they are required only to work the designated number of hours. Flex time does not lend itself well to the delivery of healthcare, because most medical facilities must be geared to appointments, timetables, and specific work shifts to ensure adequate staffing.

## Surplus or Damaged Property

Medical care facilities of all sizes continually accumulate surplus property that is damaged, obsolete, or for various reasons unsuitable for use in the current environment. A policy must be prepared that defines a procedure for the proper disposition of such property. The following is an example of a policy covering the disposal of surplus or damaged property:

*All medical center equipment or products deemed by staff to be unusable for any reason will be returned to the Director of Materials Management. No staff member will have the authority to sell or give away any medical center property, regardless of value or condition, unless authorized by the Director of Materials Management on a case-by-case basis.*

## Contraband

In this context, the term *contraband* includes not only illegal items, such as weapons, drugs, and explosives, but also alcohol. Alcohol must be included in a hospital policy

banning employees from bringing contraband items onto the facility property. The following is an example of a policy covering contraband:

*No medical center employee will possess or knowingly assist another person in possessing any contraband, including illegal drugs, explosives, weapons, and liquor of any kind, unless authorized by a supervisor for a specific medical center business purpose.*

## Drug Testing

Testing of applicants and periodic testing of staff for drug use is a commonplace procedure in healthcare organizations. The Drug-Free Workplace Act, contained in the Anti-Drug Abuse Act of 1989, spurred many organizations to action, even though the act does not require a drug testing program. The act applies to any contractor who has federal contracts for the procurement of goods or services valued at \$25,000 or more or who receives federal grants, regardless of the dollar amount. The act requires these contractors to publish a policy statement prohibiting the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance in the workplace and specifying penalties for violations; to establish an education program on drug abuse; to provide policy statements to each employee; and to require employees to report any conviction for a criminal drug violation that occurred in the workplace. When considering drug testing, all aspects of such a policy must be covered, including the type of testing and the conditions under which employees will be tested. The details of the policy must be presented to all affected individuals. Organizations should document the relationship between job performance, health and safety, and drug usage. The results of drug tests are confidential and generally should not be maintained in the staff personnel files.

## Employee Assistance Programs

Most healthcare organizations have an employee assistance program (EAP) of one sort or another. A direct relationship exists between security and EAPs. Many instances of employee wrongdoing can be traced back to personal problems. Stealing to support a drug habit is an obvious example where theft could be averted by helping a staff member with such a problem. Staff who steal because they do not understand how to manage their personal finances are a less obvious example. Even marital problems may lead to wrongdoing by a staff member that otherwise may not have occurred. An in-depth EAP effort is a way to prevent crime and wrongdoing among staff. Progressive security administrators may wish to explore this concept further with the administrator of the healthcare EAP program.

## Loss of Staff Property

Unfortunately, the loss of staff property is a continuous problem for protection systems. The provision and use of staff lockers are primary safeguards against staff property losses.

This staff property loss problem usually evolves from a lack of proper storage facilities, carelessness, misuse, or failure to use the facilities provided. An inspection of virtually any HCF—hospital, nursing home, clinic, or physician’s office—will usually reveal purses and backpacks sitting in open view, simply inviting a loss. The mandate for the security function is to provide an adequate means of storage. Failure to use the storage provided gives employees little cause for legitimate complaint if their property is borrowed, lost, or stolen.

## References

1. Supervisor blamed for rapist hire at hospital. (2009, February 10). Retrieved February 18, 2009, from [http://www.nbclosangeles.com/health/tips\\_info/Supervisor-Blamed-for-Rapist-Hire-at-Hospital.html](http://www.nbclosangeles.com/health/tips_info/Supervisor-Blamed-for-Rapist-Hire-at-Hospital.html).
2. Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to security* (8th ed., p. 304). Burlington, MA: Butterworth-Heinemann.
3. Idziak, B. (2006, January). What’s new in 2006? *Security Products*, 39.
4. HireRight reports the top five lies told by job candidates. (2009, March 8). *Campus Safety Magazine*. Retrieved March 11, 2009, from <http://www.campussafetymagazine.com/News/?NewsID=2762>.
5. Rosen, L. S. (2005, July). Criminal databases and pre-employment screening: The good, the bad, and the ugly. *Security Technology and Design*, 27.
6. Lashier, R. (2006, June). Everybody Screen! *Security Products*. Retrieved June 24, 2009, from <http://secprodonline.com/Articles/2006/06/01/Everybody-Screen.aspx>.

# Employee Involvement and Security Awareness

Crime prevention presentations, handouts, events, and training can raise staff awareness of security issues. Not only will this add eyes and ears to the security effort, it will be noted by TJC surveyors and other regulatory agencies that are increasingly looking for employee involvement in the healthcare security program. Using input from the healthcare staff, physicians, visitors, and patients, an employee involvement and security awareness program should be tailored to meet the individual needs of the facility and the employees, staff, patients, and visitors it serves.

## Employee Security Education and Motivation

The strategy of preventing crime is a key concept of the healthcare protection system. In the United States, the Crime Prevention Coalition, formed by 19 organizations in 1980, provides strong leadership for crime prevention programs. The campaign featuring “*McGruff the Crime Dog*” was one of the first efforts to involve the average person in the fight to prevent crime. The approach was unique: when people come together, work with law enforcement (or security), and address the cause of crime, they have an impact. As a result, the crime prevention and community (employee) involvement message took root. Today, the coalition is stronger than ever, and it consists of over 400 national, state, and federal organizations and community-based agencies.<sup>1</sup> The National Crime Prevention Council (NCPC) is an excellent resource for promoting a message grounded in the principles of security awareness and education and promoting the prevention-first approach to crime to employees, volunteers, physicians, and others in the healthcare environment. Training, topical crime prevention materials and strategies, media relation techniques, and other resources are available from the NCPC at little or no cost.

*Crime prevention* has been defined in many ways. The definition found in the coalition’s handbook, *Foundations for Action*, seems to be the most appropriate for the purposes of this discussion. Crime prevention, it says, is “a pattern of attitudes and behaviors directed both at reducing the threat of crime and enhancing the sense of safety and security, to positively influence the quality of life in our society, and to help develop environments where crime cannot flourish.” This is a tall order and a challenge for even the most professional healthcare security administrator.

## Employee Education Programs

A primary function of any protection system is to educate, stimulate, and motivate the first-line protection resource: employees. The protection level of a medical care facility is directly related to the extent to which employees participate in the security effort.

The entire staff of an organization must understand that they are a part of providing a safe and secure environment. They must actively practice good security awareness and appropriate security actions every day. This requires that staff be given clear direction and sufficient training and education. Security training should begin with the first day of employment and continue through to the end of the individual's service to the organization.

This participation varies from overt to covert activity. This is not to imply that all employees are engaged in overt security activities. Rather, some employees may participate by obeying the rules; for example, not taking property that does not belong to them. Other employees participate overtly by reducing inventory and thus reducing the opportunity for theft, maintaining control of keys and organizationally issued identification, marking property, reporting losses and suspicious activity, tightening procedures for identifying people in their area, greeting unknown persons in their area, and properly locking their personal belongings and work areas. All these activities, occurring simultaneously, are what a security system is all about. No healthcare administrator or security professional should be so naive as to think all employees will do their share. However, education and direction by the security department will certainly increase employee participation and involvement, obtain staff ownership in the protection effort, and engage their awareness to issues that affect the overall security posture of the healthcare organization. Common educational components include security presentation at the new employee orientation, brown bag lunch and learn programs, and department-specific in-services.

### *New Employee Orientation Presentation and Handouts*

Employee education begins with new employee orientation. New employees can be channeled into the protection system with a minimum of effort. They seek the norms and want to know what their employer expects. The moment employees first enter the workplace is the prime time to develop a positive protection attitude. Employees will not remember everything that is presented, but they will form a basic opinion, either consciously or unconsciously, of the importance that the organization places on security.

It is readily accepted by TJC and other healthcare industry regulatory agencies that healthcare employees should be knowledgeable and aware of personal safety and security issues. The security training is most effective when led by the healthcare security administrator. Typically, most healthcare organizations offer between 20 minutes to an hour to communicate the security message, based on the length of the overall orientation program. More and more frequently, healthcare organizations offer new employee orientation and specifically the security section via computer-generated learning modules.



Unfortunately, many healthcare organizations have combined the security presentation with safety and emergency management and the important codes every healthcare employee must know. Although the healthcare employee is given a basic exposure to security and the protection efforts employed, most healthcare security professionals agree that the same effort that goes into promoting patient safety and infection control should be applied to protection and the security awareness message. The IAHS has a basic industry guideline for general staff security orientation and education that should be implemented in every healthcare facility.

#### IAHS—HEALTHCARE BASIC SECURITY GUIDELINE, #03.02

##### **General Staff Security Orientation and Education**

**STATEMENT:** Healthcare facilities (HCF) will identify the security orientation and education needs of general staff. “General staff” is defined as all personnel regularly serving the HCF. Based on the orientation and education needs identified, the HCF will implement a program to provide this information.

##### **INTENT:**

- a. Expectations of how staff contribute to a safe and secure environment should be explained, including how staff contact Security; what information staff should report to Security; the importance of displaying and checking identification; procedures for preventing and responding to infant/child abductions; preventing, intervening in, and resolving workplace violence issues; crime prevention; personal safety awareness; and confidential information such as HIPPA requirements.
- b. Security orientation and education should be presented to all HCF staff within thirty (30) days of employment with periodic reviews and updates of information at least annually.
- c. Security-sensitive areas have special staff orientation and education needs. If assigned to a security-sensitive area, such special training should begin on the first day.
- d. The HCF should determine and continuously evaluate the method of presentation which best accommodates staff needs. Presentation may include classroom, video, newsletter, role playing, drills, and electronic self-learning education modules.

**Approved:** December 2006

To offset lack of time provided during new employee orientation and facilitate enhanced employee knowledge of the security effort, there should be a handout for the new employee emphasizing the importance of security to themselves and the organization. Progressive security programs distribute a small book or pamphlet that describes the basic elements of the security program and serves as a quick reference to the services and resources offered by the security program, including employee expectations in terms of providing safety and security. These booklets can be purchased and customized for the

**Table 15-1** Basic Listing of Security Services and Resources**Security Services and Resources Offered by Protection Department**

- Responds to security incidents and documents follow-up actions
- Identifies security risks and vulnerabilities
- Responds to requests such as locking or unlocking doors, vehicle assistance, patient assists, and visitor services
- Investigates hospital incidents:
  - unsafe conditions
  - missing property
  - suspicious activity
  - vandalism
  - accidents
- Assists with the control of visitors, patients, and unauthorized persons
- De-escalates aggressive or crisis situations
- Assists staff in controlling unruly or violent persons under clinical supervision
- Responds to alarms
- Physical security of work area
- Escorts people, cash, and valuables
- Coordinates activities with law enforcement and public safety agencies
- Offers educational programs to employees and staff
- Provides loss prevention awareness
- Conducts security well-being checks for employees and staff members working late and working in a department alone
- Detains law-breakers and assists with court action, as warranted

healthcare facility or created with in-house resources. [Table 15-1](#) is sample listing of the security services and resources often shared by the protection professional during the new employee orientation program.

Few organizations use security competencies in the organization's annual competency requirements; however, of the organizations that do, they have found success using self-learning packages. This approach enables employees to study the material on their own and demonstrate their knowledge through a competency exam. The self-learning package is typically limited to the important security issues that employees are expected to know and demonstrate on an everyday basis such as reporting security events, the role of customer service greetings in the security effort, infant/child abduction employee response, etc.

#### *Department-Specific Security Training Programs*

Healthcare organizations are traditionally heavily involved in a continuous program of in-service education. Security administrators should take advantage of every opportunity to involve protection services in these educational programs through departmental meetings or small group meetings. At one medical center, the entire workforce is subjected to a general in-service program on a quarterly basis. Security training for general staff can be provided by various entities, including human resources, security administrators, in-service education departments, and risk management personnel.

**Table 15-2** Employee Awareness Campaign Topics

Crime Prevention/Employee Awareness Educational Program Topics	
<ul style="list-style-type: none"> <li>• Building a Personal Safety Plan</li> <li>• Workplace Violence Prevention</li> <li>• Front Desk Safety: A Program for Volunteers</li> </ul>	<ul style="list-style-type: none"> <li>• Senior Safety: An Anti-Crime Guide</li> <li>• Safeguard Your Child</li> <li>• Personal Safety for the Healthcare Community Worker</li> </ul>

Self-directed security presentations with audio have been successfully used at many healthcare facilities. These programs are designed to explain a variety of critical information that every employee should know such as workplace violence prevention and reporting, bomb threat response, or other department- or function-specific educational programs such as front-desk security or what to do in the event of an armed robbery (gift shop, pharmacy, or other cash-handling area). Computer-generated learning modules can be produced in-house using a basic PowerPoint presentation with voice narration, recorded webinars, or off-the-shelf products purchased from professional trade associations such as IAHSS, ASIS International, or other outside companies.

#### *Crime Prevention and Personal Safety Classes*

Special classes provide another opportunity to tell the protection story. Because medical care facilities employ many female personnel, personal safety and self-defense classes are popular. A broad range of security information can easily be included in special classes. Hosting a regular series of brown bag lunch and learn programs are popular with many organizations with employee-focused protection campaigns as well as community outreach programs for seniors. Potential themes for these types of programs include those listed in [Table 15-2](#).

### Crime Prevention/Employee Awareness Activities

Professional security administrators must seek new ways and new opportunities to communicate with employees. This activity yields a high return for the time and money expended. There are various methodologies outside of direct education which the healthcare security program can utilize to solicit the assistance of staff members as well as increase their awareness of security-related issues. These components include healthcare facility newsletter submissions, security handouts and pamphlet distribution, departmental websites and seasonal and time-sensitive e-mail broadcasts, security fairs, and other methods to communicate the security awareness/employee involvement message.

#### *Newsletters*

Medical center newsletters are good mediums for educating employees. Most newsletter editors are continually looking for new material. Because the protection effort is of general interest to employees, the security administrator generally finds that such material is

**Table 15-3** Security Newsletter Topics

Crime Prevention Corner Newsletter Themes	
<ul style="list-style-type: none"> <li>• Auto Theft Prevention</li> <li>• Robbery: Prevention and Reaction</li> <li>• Planning for Emergencies</li> <li>• Bicycle Safety</li> <li>• Vacation Security Checklist</li> <li>• Crime Prevention for the Elderly</li> </ul>	<ul style="list-style-type: none"> <li>• Protecting Kids on the Internet</li> <li>• Home Security</li> <li>• Personal Identity Protection</li> <li>• Halloween Safety</li> <li>• Back-to-School Safety</li> <li>• Neighborhood Crime Prevention</li> </ul>

welcomed. Security information may be published randomly or in a regular column such as a “Crime Prevention Corner.” Newsletter themes often include personal safety issues at work and at home and include such topics as those identified in [Table 15-3](#).

### *Security Handouts*

Color posters, tri-fold brochures, and table tents are common methods of educating employees about security. In medical centers, posters have traditionally been used for safety messages, but they can be used to convey other messages as well. Visitor and staff elevators are often used for posting information. In other programs, bulletin boards located near the cafeteria or other common public corridors have been dedicated to the security department for posting of security awareness information.

The distribution of handouts and use of table tents in the cafeteria are excellent tools to remind employees of the importance of general security awareness during seasonal times such as the holiday season or daylight savings time. Figures 15-1, 15-2, and 15-3 provide three examples of handouts and table tents that can be used in the protection program to keep security awareness at the forefront in the minds of healthcare employees.

Handbill notices are another way to deliver short messages to employees. Handbill notices can be distributed at employee orientation sessions, at periodic employee in-service programs, to nursing stations and operating departments, or as a payroll insert. [Figure 15-4](#) is an example of a handbill notice.

### *Websites and E-Mail Broadcasts*

Security events or information relevant to the entire campus can be shared via a link to the healthcare organization’s internal website or via an e-mail distribution list. A dedicated protection program website can be used to:

- Remind employees how to report a security incident or suspicious activity;
- Keep the healthcare community abreast of new developments/improvements made in the security program;
- Help prepare employees for upcoming TJC surveys and potential security-based questions frequently asked by surveyors;



FIGURE 15-1 Crime takes no holiday.

- Identify specific security department performance standards, goals, and improvement initiatives;
- Provide answers to frequently asked questions in the security program such as the role of an employee in a bomb threat, how to obtain a replacement identification badge, etc.;
- Offer a biography of the security staff;
- Present status reports on security initiatives that are being carried out in the facility, such as new video surveillance installations, results of employee surveys, changes to parking policies, etc.;
- Describe the role and responsibility of each employee with the hospital in respect to maintaining a safe and secure environment;
- Calendar of security awareness education programs offered.

Some healthcare protection departments post the CAP Index map and site data (see *Chapter 8, Security Attire and Equipment*, Figure 8-6) on the internal website to enhance employee awareness of the probability of crime to occur in the neighborhood surrounding the facility, while others post annual police crime statistics. In general, the information posted is limited only to the creativity of the healthcare security administrator and his/her desire to communicate with employees of the organization.


Seasonal and time-sensitive e-mail broadcasts are effective tools during holiday or vacation seasons reminding employees of good security awareness habits and techniques.



**MAKE  
SECURITY  
AWARENESS  
A  
NEW YEAR'S  
RESOLUTION**

- *Be aware of your surroundings at all times.*
- *Be alert for strangers. If their identity or business is unknown, ask if you may help.*
- *Encourage patients to send belongings and valuables home with a family member or secure valuables in the hospital safe.*
- *Report suspicious activity and all losses, regardless of how minor, to security.*

FIGURE 15-2 Make security awareness a New Year's resolution.



***Father Time is Rolling Back His Clock Again.***

*with Daylight Savings  
time ending,  
you'll be spending  
extra time in the dark*

***If You're Parked In A Remote Area, Walking  
Alone, or Feel Uncomfortable;  
Call Security For An Escort.***

***We're Here When You Need Us.***

FIGURE 15-3 Reminder to staff about using escorts with daylight savings time ending.



**WE'RE HERE WHEN YOU NEED US....**

## **SECURITY ESCORTS**

During normal shift change hours officers are regularly assigned outside to offer maximum protection for all employees. If you leave work either before or after these times, call for an escort.

To request an escort call security a few minutes prior to your departure. An officer will be dispatched to escort you as soon as possible. However, response time may vary due to other responsibilities.

Please utilize hospital parking lots as off-property escorts are limited to one block.

**Ext. 6608** **WE CARE ABOUT YOU!**

Healthcare Security Services

**FIGURE 15-4** Example of a crime prevention/security awareness handbill.

Additionally, e-mail broadcasts can be used effectively after a serious security event at the facility or in the surrounding neighborhood to help with rumor control and to foster good employee relations. A healthcare facility in Aurora, CO, used e-mail notification to bring employee and staff attention to a disturbing trend of auto thefts/break-ins occurring on campus. In the e-mail message, security leadership was able to share a common thread for each of the incidents that included doors being left unlocked or keys found in the ignition. The use of these e-mail broadcasts helped put an end to the events.

For both websites and e-mail broadcasts, the protection professional should review all available content with the healthcare facility's public relations and/or marketing department prior to posting or dissemination. This will help ensure that inappropriate content is not shared inadvertently or create undue concern due to the perception of personal safety on campus.

### *Other Considerations*

Other methods used to keep security issues front and center in the healthcare environment include town hall meetings organized by administrative or nursing leadership. Participation in these meeting allows security leadership an opportunity to highlight specific information and address issues directly.

The security fair is another popular crime prevention activity. They have proven quite successful and generally draw more than 75% of the total employee workforce when effectively organized and promoted. Pens and pencils carrying various security themes are distributed with scratch pads that have the security telephone number. Door prizes and food always boosts attendance.

## **Security Knowledge for Every Healthcare Employee**

Security involves everyone in the healthcare facility. The eyes and ears of every employee are essential to the safe-keeping of the healthcare environment.

An important aspect in the protection program is to involve healthcare employees and staff in the communication and reporting of events or suspicious persons to the security department, customer service greetings, and the availability of security escorts, parking lot security, and the employee's role in the basic crime triangle.

### *Reporting Incidents*

Employees should be requested and guided by organizational policy to report all missing property, acts of vandalism, or other unusual occurrences to the security department without delay.

All calls to security should be answered by a staff member who remains in constant contact with patrolling security officers via two-way radio or other means of communication. When calling for security assistance, the healthcare employee should be encouraged to provide the following information:

- **NAME:** name of the requesting party
- **NUMBER:** where they are calling from
- **NEED:** the service needed and location of the request

This information should be requested in case additional contact with the requesting party becomes necessary. If a telephone is unavailable, employees should be instructed to observe and document suspicious persons or activities. In such instances, employees should be encouraged to obtain security assistance by requesting a fellow staff member to call for or physically obtain a security officer. In selected work areas, duress alarm systems have been installed and can be used to summon security assistance in emergency situations. Employees in work areas where duress alarms are located should be instructed to activate the alarm only when it is safe to do so. Once the alarm has been activated, follow up with a telephone call to security to verify the alarm and provide the dispatcher (or PBX operator) with additional information.

The need for reporting security incidents was a difficult lesson to learn for one Midwestern hospital that experienced three sexual assaults in one night. Like many hospitals, the organization required visitors to sign in and wear temporary issued identification badges after standard visiting hours. But the organization did not strictly adhere to this policy. It was not unusual for nurses and other staff to see strangers walking the halls at all hours of the day; staff rarely challenged unauthorized persons or notified security of their presence. Unfortunately, the hospital had an assailant enter the hospital after visiting hours and spent many hours becoming familiar with the layout and design of the facility. A Centers for Medicare & Medicaid Services (CMS) survey conducted within weeks after the incident found many deficiencies in safety and security, including the failing of the hospital to preserve patient rights, failing to ensure safety, and failing to follow its own policies. CMS gave the hospital just 6 weeks to address the deficiencies or risk having in Medicare participation status revoked.<sup>2</sup>

There are several lessons learned from this incident for the healthcare security administrator. These lessons include the importance of the hospital-issued identification,



awareness of strangers versus suspicious persons, and the use of secret shoppers in the protection program to validate employee involvement and the need for continual security awareness.

### *Customer Service Greetings*

Awareness and greeting of all persons who frequent a unit or department is a very effective approach to involve employees in the crime prevention effort. The simple acknowledgement of others is a proven technique for deterring crime and unwanted behavior. If someone's identity or business is unknown, the employees should be expected to ask if they may help them. If an unsatisfactory reply to the question is received, or if suspicious activity is observed, or if the employees or volunteers are simply uncomfortable with approaching the person, they should be instructed to contact security immediately.

### *Security Escorts*

Every healthcare security department should provide a personal escort service for patients, staff, and visitors. Security officers should be alert to anyone walking alone to a remote area or encourage the use of escorts for anyone who "just feels uncomfortable." The education component should encourage requests for a security escort to include a few minutes' lead time to minimize their wait and potential frustration.

During major shift changes, security officers should normally be deployed to provide exterior protection, therefore reducing the necessity of individual escorts. Security education should inform employees of this basic deployment expectation and encourage them to use the buddy system and walk with others.

### *Parking*

Most healthcare campuses have parking areas to accommodate patients, staff, and visitors with designated parking for each. Employees should be encouraged to always park in well-lit, heavily traveled parking areas, locking their doors, and not leaving valuables in their vehicle. To minimize the opportunity for crime, employees should be encouraged to reduce the visibility of their personal property by utilizing the vehicle's trunk.

The protection and safeguarding of parking areas, including garages, are discussed in more detail in *Chapter 23, Parking Control and Security*.

### *The Crime Triangle*

There are three basic elements necessary for a crime to occur: a criminal with the DESIRE and ABILITY to commit a crime and a victim who provides an OPPORTUNITY for the crime. Healthcare facilities, by their very nature, can afford ample opportunities for crime. [Figure 15-5](#) shows the interrelationship of the three basic elements of the crime triangle.

Involvement and participation of employees in security awareness activities can be one of the most cost-effective components of the healthcare protection program. Court-certified experts in healthcare security have routinely found that the most frequent



FIGURE 15-5 The crime triangle.

common denominator in hospital security lawsuits is employee apathy and inattentiveness. All too frequently, aberrant behavior is not recognized or brought to the attention of the security staff.<sup>3</sup>

Employees can do a great deal to reduce the opportunity for crime in the hospital. The most effective defense against crime is common sense, alertness, and basic precautions. Helpful tips for employees include:

- Always wear proper hospital identification. This identification helps patients, staff, and security recognize authorized personnel.
- Be aware of your surroundings at all times. Be familiar with regular employees in the work area and question unknown persons.
- Many losses are a result of carelessness. Maintain security of personal effects and hospital property. Whenever possible, carry only those items that you will need. Always minimize the amount of cash and number of credit cards you carry. If you bring a purse, never leave it in plain view—secure it in a locker or a lockable cabinet. Always secure storage cabinets and work areas when unattended.

### Perception of Safety and Employee Attitudes

Healthcare organizations have found it extremely important to determine employee attitudes concerning their work environment. A positive attitude of support and appreciation of the security effort is essential to providing a safe and secure environment. A common method to assess such employee attitudes is to hire an outside firm that specializes in employee surveys. These firms generally use standard questions, but allow the organization being surveyed to develop some specific attitude questions. When security questions are used in these surveys, they should be very specific. If a survey produces a slightly positive or a neutral response, it should be considered extremely good because

<i><b>Security Incident &amp; Officer Response Evaluation</b></i>		Hospital	_____		
		Dept	_____		
		Date	_____		
		Officer(s)	_____		
			_____		
Please complete the following evaluation to assist in evaluating the security officer's response					
	<i>1 – did not meet expectation</i>	<i>3 – met expectation</i>	<i>5 – exceeded expectation</i>		
Officer(s) Responded Promptly	1	2	3	4	5
Officer(s) Appropriately Addressed and was Effective in Handling Situation	1	2	3	4	5
Officer(s) Maintained Dignity & Respect of All Parties Involved	1	2	3	4	5
Other Comments					
_____					
_____					
<b>THANK YOU</b>					
<i>Please drop off your evaluation in the mail or the Comment Box located outside of the Security Office</i>					

FIGURE 15-6 Security services performance survey.

many employees have been victims of incidents, have received parking violation notices, or have a general disregard for the authority that security represents.

Another method of measuring the attitudes of employees is to conduct an in-house survey. One hospital obtained good results by approaching a local college and having the survey conducted by students as a class project. The class acted as a third-party surveyor and tabulated and analyzed the results.

Surveying the attitudes of employees must be an ongoing endeavor. Figure 15-6 is an example of a form utilized in one program in an ongoing effort to measure the performance of security personnel. In this program, completed Security Incident Reports and Security Condition Reports are utilized to send a random survey form to a recipient of a specific service or incident. This form is a prestamped mailer that is sent back to security for analysis and the formulation of improved service plans if appropriate.

Survey results are the basis for recognizing outstanding service, the need for training, and a review of operating procedures. This measurement tool can be very useful in comparing one facility with another. This type of performance measure fits in with TJC accreditation standards and is ready-made to help security personnel develop a performance improvement program.

## Hospital Watch

The term *hospital watch*, which refers to an approach to hospital crime prevention, was adopted from the neighborhood watch programs promoted by local police agencies.

Hospital watch can take on many different forms. It is a generic approach to involving the hospital community in observing, reporting, and dealing with suspicious activity. Because there are no specific guidelines or program elements, the activities of this program are limited only by the ingenuity of the security administrator.

## References

1. National Crime Prevention Council. Crime prevention coalition of America fact sheet. Available at <http://www.ncpc.org/programs/crime-prevention-coalition-ofamerica/cpca%20fact%20sheet.pdf>. Retrieved on June 16, 2009.
2. Sexual assaults lead to security overhaul. (2009). *Environment of Care Leader*, 14(9), 1, 3–4.
3. Nesbitt, W. H. (2009). Avoiding security litigation in a healthcare setting. *The hospital security reporter*. SMSI online newsletter. Available at [http://www.thehospitalsecurityreporter.com/articles/09\\_0423.html](http://www.thehospitalsecurityreporter.com/articles/09_0423.html). Retrieved on June 11, 2009.

## Investigative Activity

Investigative activity is a major component of any healthcare security program. It involves gathering and evaluating facts (including evidence) for either criminal or business (corporate) purposes. The techniques and purposes of a business investigation are much broader and more complex compared to the traditional law enforcement investigation. In addition to investigating crimes or alleged crimes, security personnel may gather information regarding the violation of organizational rules and regulations; a job applicant's background; alleged harassment; alleged discrimination; conditions that may lead to criminal violations; the need for new security controls and procedures; liability claims or potential claims; unsafe conditions; or evidence needed to prove or disprove certain allegations against the organization. Furthermore, a security investigator is in the best position to determine why a problem occurred and make recommendations regarding crime prevention and how to prevent the problem from occurring again.

A law enforcement investigation, on the other hand, is conducted basically for the purpose of apprehending the perpetrator of a crime and obtaining the evidence required to successfully go forward in prosecution of the case. In short, healthcare security investigations are more varied and often more unique than law enforcement investigations. Also, the objective of an investigation may be different even when the healthcare organization has a strong policy of prosecuting those who violate the law; the end result may be an organization administrative remedy rather than a criminal court proceeding. Often, the investigator who has put in time and effort and uncovered information regarding a perpetrator engaged in a criminal act would like to pursue prosecution. However, healthcare administrators must be allowed to make the decision regarding prosecution. The investigator must subordinate their desires to the administrator making the final decision.

The style of an investigation is shaped by organizational philosophy, the purpose of the investigation, risk to the organization, as well as the background and traits of the investigator. The organization's security department will generally handle investigations unless there are major losses to the organization and/or there is suspected white-collar crime or wrongdoing by administrative or upper-echelon principals of the organization. When it is determined that an outside investigative agency should be hired to conduct an in-depth internal investigation, it is common to engage legal counsel to oversee the methods and processes of the investigation.

Investigations conducted by the healthcare organization may be performed for a variety of reasons and by a number of different departments or combinations of

departments. As an example, Risk Management conducts investigations into operational matters such as patient care complaints, insurance claims administration, medical practices, and events required by accreditation or regulatory agencies. Healthcare organizations can even be fined by regulatory agencies for not investigating an alleged incident. Such was the case for a California hospital that was fined (sometimes referred to as an administrative penalty) for not promptly investigating an alleged sexual assault by a staff member against a patient. The fine was leveled by the California Department of Public Health, which licenses approximately 450 acute care hospitals throughout the state.<sup>1</sup> Some states in their criminal code have a duty to report a crime. The state of Colorado in Section 18-8415 of its criminal code “duty to report a crime – liability for disclosure” states that it is the duty of every corporation or person who has reasonable grounds to believe that a crime has been committed to promptly report the suspected crime to law enforcement authorities.

## Fair Credit Reporting Act (FCRA)

The FCRA is an American federal law that was passed in 1970 and is enforced by the US Federal Trade Commission (FTC). The law contained certain provisions that required certain “notice” and “disclosure” information be given to individuals relative to certain investigation and inquiry into the individual’s credit situations. In 1999, the FTC rendered an opinion that such notices and disclosures were required if an employer used outside investigators in cases of suspected employee misconduct. This meant that the employee suspected of misconduct had to be notified before any investigation could take place. The ramifications of giving the employee the opportunity to destroy evidence, tamper with evidence, and/or influence or threaten witnesses were a huge factor in promoting misconduct and various crimes. Sanity returned several years later when the President of the United States signed the bill reauthorizing the FCRA. The bill removed the provision of notice in the cases of misconduct investigations. This removal continues to allow employers to hire outside experts to investigate incidents of workplace misconduct without fear of liability.<sup>2</sup> Even though notification of the employee provision was removed, an outside investigator with no connection to the healthcare facility tends to be more impartial and in a better position to protect the employee’s interest.

## Security Versus Police Investigation

The many types of security investigations required in the healthcare facility can be as complex as the function of providing medical care itself. The majority of conditions or incidents that require investigation are noncriminal, or of such minor criminal status, that law enforcement agencies are virtually unconcerned with them. If every incident legally classified as a crime were reported to a law enforcement agency, a crime wave would appear to take place. The number of crimes reported to the police by an organization, and the community as a whole, is many times less than the actual number of crimes committed within any organization or community.

It is also somewhat common for the Security Department to be actively investigating the circumstance of a crime in parallel to the ongoing law enforcement investigation of the same incident. The objective of each investigation may be different or the objective may be the same. In any case, the security investigation must be conducted in such a manner that it does not interfere or jeopardize the criminal investigation being conducted by law enforcement. The best way for the security investigator to make sure they do not interfere with the police investigation is to make contact with the office in charge of the case and review the circumstances regarding the security investigator's involvement. Often, the security investigator and law enforcement officer/detective can collaborate, resulting in a successful conclusion to the case.

### Concern for Minor Crimes

The so-called minor crimes that are not reported to the police are of concern to a medical care facility for a variety of reasons. Even the incidents of minor crimes may give a health-care organization a poor image to the public and staff. Further, such crimes may be only the surface of a larger crime problem and thus always deserve an investigative response to evaluate the extent of a situation and the potential need for an in-depth investigative process. Also, not all incidents reported to security are crimes. In fact, many property losses can be traced to the loss of accountability of the property or false reporting rather than actual theft. Consider some specifics. An all-too-common problem in healthcare facilities is the loss of personal property of patients. Although many losses of patient property do occur, most incidents involve small items or cash in small amounts. These losses are generally not reported to the police because it is simply unrealistic, given the limited amount of police resources. On the other hand, the loss of patient property is of major concern for the organization. Another type of loss of little or no interest to law enforcement agencies is the disappearance of a key to a critical area of the facility. The police would not become involved unless the key is used to commit a crime. A significant part of a security investigator's work is determining whether a crime has actually occurred. An objective of the security investigator working the incident of the missing key would be to conduct an inquiry to ascertain whether the key was misplaced, lost, or stolen. If the facts point strongly to the latter, the investigator might recommend changing the locks or setting up a surveillance of the affected area. Neither of these alternatives would normally relate to law enforcement involvement. Regardless of whether the security investigator is successful or not in resolving the problem, a follow-up ensures good public/employee relations. It indicates to a victim that the organization cares enough to provide additional support to make every effort to resolve the problem. This is especially critical concerning patient valuables. A security investigator following up on missing patient property indicates to the patient how much the organization cares.

### Types of Investigation

We have already discussed the need and general aspects of healthcare security investigations. These investigations can be divided into operational investigations of security

incidents and the more sensitive, or higher-level, investigations. The operational investigation typically begins when the security officer is dispatched to respond to a specific situation (vandalism, theft, property damage, disturbance, threatening behavior, etc.). The second type of investigation involves significant or suspected ongoing misconduct, such as embezzlement, sexual harassment, drug abuse, fraud, and kickbacks. This type of investigation may involve utilization of outside investigators. There are various advantages to using an outside investigator, including added expertise, resources, and timeliness. An outside investigator tends to be more objective and impartial. Planning for the process and authorization to conduct higher-level, and possibly sensitive, investigations should take place before the need arises. The healthcare security administrator should seek out at least one outside investigative resource as part of a sound strategic plan. It takes time to interview investigative firms, check out references, assess capabilities, explore pricing and methodologies, determine a “fit” to the healthcare environment, and to establish clear understanding of philosophies of both the buyer and the provider of investigative services. Selecting a vendor in advance of the specific need will save time when services may be required on a short notice. In any investigation, the goals and objectives of both the outside investigative organization and the healthcare organization must be mutually agreed upon and clearly documented. Details to be agreed upon include projected costs, reporting protocols, timetables, and the processes for maintaining control of the investigation. The investigation should be continually monitored and managed with accurate and timely feedback relative to the investigative effort. It is certainly helpful if the outside investigator has prior experience in dealing with the protocols, policies, and procedures of the healthcare environment. The IAHS has general investigative guidelines that it has developed for healthcare organizations investigating security incidents, alleged crimes, and other situations that may involve injury, loss, or damage.

#### IAHSS HEALTHCARE BASIC SECURITY GUIDELINE, #04.01

##### **Investigations—General**

**STATEMENT:** Healthcare facilities (HCFs) will develop procedures for investigating security incidents, alleged crimes, incidents involving injury, loss, or damage, and for administrative purposes.

##### **INTENT:**

- a. Investigative actions refer to the impartial observation and gathering of facts and information for criminal and noncriminal purposes.
- b. Facility staff, including security personnel, may engage in investigative activity for a variety of purposes and situations, to include:
  1. To determine if there is criminal activity
  2. Safety-related incidents/accidents



3. Audits of control procedures
  4. Suitability of applicants seeking employment
  5. Reducing the likelihood of future incidents
  6. Assisting law enforcement or other public safety and regulatory agencies
- c. Facility staff conducting investigations should have a basic understanding of the difference between a criminal and a noncriminal investigation. This understanding should include policy and procedure for reporting facts and findings to law enforcement at an appropriate point when, and if, investigative activity indicates suspected criminal activity.
  - d. The investigation of an incident should be undertaken as soon as practicable and procedures should be in place to preserve an incident scene and other evidence where indicated.
  - e. Security investigations of a criminal nature should be conducted in a manner that does not interfere or jeopardize a law enforcement investigation.
  - f. The depth and complexity of an investigation will depend on the frequency and severity of an incident or combination of incidents.
  - g. Investigation of security incidents may include overt, covert, or a combination of these activities.
  - h. Security officers who observe a security incident, or who have been dispatched to the scene of an incident, shall complete a security report relative to their investigation/ activity prior to the termination of their respective shift.
  - i. The investigation and/or control of a security incident may be ongoing and, through established procedure, may be “passed off” from officer to officer and shift to shift.
  - j. There should be a policy and procedure for administrative/supervisory review of security officer incident reports for completeness of the report, and to determine the need for any further investigative activity of the incident.
  - k. There should be a policy and procedure concerning investigative results relative to documentation and sharing with internal or external departments and agencies.

**Approved:** November 2007

**Last Revised:** October 2008

## Incident Investigations/Two Phases

Incident investigations generally have two distinct phases. The first phase, generally referred to as the *preliminary investigation*, is usually conducted by field security officers. This first phase is also sometimes referred to as the *initial investigation*, which may resolve the matter and thus there will be no need for further investigative activity. A preliminary investigation is conducted up to the point at which postponement of further investigation will not jeopardize the successful conclusion of the case. O. W. Wilson, one of the greatest police executives the United States has known, defined preliminary investigation over

a quarter of a century ago. It is a definition that remains current today. He defined it as follows:

<b>P</b>	Proceed to scene with safety and dispatch
<b>R</b>	Render assistance to injured
<b>E</b>	Effect arrest of perpetrator
<b>L</b>	Locate and identify witnesses
<b>I</b>	Interview complainant and witnesses
<b>M</b>	Maintain scene and protect evidence
<b>I</b>	Interrogate suspects
<b>N</b>	Note all conditions, events, and remarks
<b>A</b>	Arrange for collection of evidence
<b>R</b>	Report fully and accurately
<b>Y</b>	Yield responsibility to investigators or higher authority <sup>3</sup>

One of the most important considerations during a preliminary investigation is to proceed to the scene as quickly as possible. How well the preliminary investigation is conducted and how quickly it is initiated have a direct effect on the probable outcome of the investigation. A prompt arrival at the scene by the security officer and/or investigator enhances the possibility that evidence will not be tampered with or destroyed. Witnesses will still be present, and they will have less chance to compare what they saw, which in turn decreases the possibility for error. Thus, a security officer responds to the incident scene to conduct an inquiry and take appropriate action. Security officers should remember that a report is only the documentation of action taken and the collection of information (facts) concerning the incident.

The second phase of an investigation is the *follow-up investigation*, or in some cases it is simply referred to as a continuing or ongoing investigation. It may begin immediately after the preliminary investigation or it may be days before further action is taken. Regardless of the time interval, a follow-up to the initial report is generally required; however, a supervisory review may be all that is required of some reports, at which time the investigation is termed inactive or closed. In small security organizations, the follow-up activity may be conducted by the same person who handled the preliminary investigation, or the security administrator may also function as the department investigator. An objective of the follow-up investigation is to obtain additional information, and at the same time, it creates a favorable image for the public and staff. Another aspect of the follow-up investigation is that it may shorten the preliminary investigation required and allows security field personnel to return to patrol, making them available for further service to the organization.

Follow-up investigators generally have access to records, files, and sources of information not available to preliminary investigators. Because follow-up investigation is centralized, specialized techniques may be used and past incidents that may have a relationship to the incident under investigation may be analyzed.

## Interrelationship of the Preliminary and Follow-up Investigation—A Typical Case

A patient informs the charge nurse that she cannot locate her expensive gold bracelet that was in her bedside cabinet at 5:30 P.M. It is now 10:30 P.M. The charge nurse notifies security, and a patrol officer is dispatched to conduct a preliminary investigation. After a thorough search of the room and the soiled linen-collection area, the officer completes the report, addressing all the basic questions (basic interrogatories of who, what, when, where, why, and how). Several possibilities exist concerning the whereabouts of the bracelet: (1) The patient misplaced the bracelet, even though the search failed to locate the property. (2) An employee found the bracelet and has, against hospital policy and procedure, locked it up for safekeeping. (3) An employee, another patient, or a visitor has stolen the bracelet. (4) The patient's family or friends have taken the bracelet home for safekeeping. (5) The bracelet was discarded unknowingly and accidentally by the patient or staff. (6) The bracelet was checked in as patient valuables. (7) There was never any bracelet in the patient's possession.

At this particular hour of the evening, the security officer does not have access to admitting records. Good judgment would preclude contacting the family late at night. The police would probably not be called until most of the above possibilities could be eliminated, providing a greater indication that a theft had, in fact, occurred. Thus, the security officer must gather all the information readily available and forward the report to the appropriate person to initiate the follow-up investigation. The follow-up investigator should start by recontacting the patient. The investigator can obtain additional information from the patient and can find out whether the bracelet had been located between the time of the preliminary investigation and this follow-up investigation. This contact allows the investigator to begin with current information or, if the bracelet was found, to close the complaint. The follow-up contact assures the patient that the hospital is concerned and that the matter is not being ignored.

## Results of Inadequate Investigations

Poor investigative response to patient-involved security incidents leads to the frequent complaint that patient concerns are not heard and the hospital does not really care. In some facilities, the nurse prepares an unusual incident report instead of directly notifying security. This is an unacceptable practice and generally results in a poor reporting process. In this respect, the process is not timely and such reports generally lack sufficient information to affect a successful resolution of the matter. In the case of the missing bracelet, it is doubtful whether the nurse-prepared report would include the last time the bracelet was seen, whether the patient received visitors during the ensuing time period, and the identity of unit personnel on duty during this time period. Unless unduly delayed, the unusual incident report passes through the nursing service office and reaches the appropriate administrative person several days later. Frequently, no follow-up action is taken and the report is simply filed for statistical purposes. Most hospitals have patient representatives, and these individuals are often the first responders to patient complaints such as missing

patient property. The patient representative often does an excellent job of gathering the initial details and is a good resource regarding follow-up investigations by security personnel. The unusual incident report may also end up with the risk manager, who again generally lacks the resources for a thorough follow-up. In short, security should be notified and conduct an investigation and prepare a report in a timely manner. It is important that the first security responder to an incident has a major responsibility to capture information that may be forever lost with the lapse of even a minimal amount of time. The importance of this information may not “register” with the investigator at the time, but may be very important at a later time. In this respect, sketches prepared and/or photos taken at the time of the incident can be helpful. A brief example of a photograph taken that proved invaluable involved the fall of a visitor down the steps of a front entrance to the facility. The visitor received injuries that required extensive surgery and the significant loss of income from being unable to work. In the litigation case that followed many months later, the visitor claimed that there was an excessive buildup of snow and ice on the steps. A photo taken of the steps at the time of the initial investigation showed dry and clean steps. The photo was a critical component of the preliminary security incident report.

### Patterns of Wrongdoing and Suspects

A major reason to encourage employees to report all incidents of wrongdoing is that sometimes incidents cannot be resolved individually, but they can be resolved in combination. Skilled investigators seek out and recognize emerging patterns that point to suspects or the probability of a repeated act. The investigation then shifts somewhat from gathering facts to setting up a plan of action, which may include surveillance or even a covert operation. Investigators often use electronic equipment (closed-circuit television, video recording, alarm devices, etc.) and various dusting powders or ultraviolet light techniques. The “planting” of an object that has been the subject of theft is also a common method of resolving problems. A possible disadvantage to this procedure is that it may induce a person to steal, but it may not be the person who has been responsible for the previous incidents under investigation. Regardless of the methods used, the resolution of incidents not only identifies perpetrators and detects system failures, but it also sends a strong message to future malefactors. However, when conducting a covert operation, permission must be obtained from the administrative staff, which may sometimes include human resources.

### Nonincident-Driven Investigative Activity

Not all security investigations involve incidents or suspected wrongdoing. Good security programs go a step further and conduct various other types of investigations to include applicant/promotional background checks, audits, spot checks, and various employee issues.

#### *Background Investigations*

In some security systems, a criminal history record check is a routine step in the employment process. In others, security is called on to perform a background check only for

particular positions or when there are specific background questions that need to be explored in more detail. This type of investigative activity is almost always performed in collaboration with the Human Resources department.

### *Audits*

Another type of investigation is sometimes referred to as an *audit*. One type of audit is a check of certain areas or activities to determine whether crimes are occurring or to determine the level of security safeguards and their effectiveness. This type of investigation, as important as it may be to the organization and the safety of patients and staff, is difficult to accomplish. The very nature of leadership of healthcare provider organizations is to tread lightly on the professional caregiver and clinical support personnel. The physician, the pharmacist, the laboratory director, and like persons expect, and enjoy, little oversight of their conduct and services from a security point of view. A case in point is the drug addictions of medical professionals who obtain “their supply” from the healthcare organization and often at the expense of pain and suffering of patients.

A recent Colorado report indicates that medical professionals with drug addictions have increased by 20% in 1 year (2008–2009) and federal agents are investigating more thefts by Colorado healthcare workers as of July 2009 than they handled in total the previous year. Peer Assistance, a Colorado nursing assistance program, worked with 84 dentists, 84 pharmacists, and 200 nurses in 2008—an increase of more than 20% over 2007.<sup>4</sup>

An audit team of an organizational auditor, a nursing supervisor, and a security investigator is essential to providing for the security and safety of the organization, the patient, and the staff relative to the area of drug control. It cannot be left to the Director of Pharmacy alone to maintain control of drugs throughout the organization, and particularly at the point where drugs are actually administered.

Another form of the security audit is to determine whether policies and procedures are being followed. Simply having a policy and procedure does not ensure compliance. In fact, noncompliance, or partial compliance, may be false security.

In addition, investigators examine procedures or operational areas to determine whether there is potential for loss and if established procedures are being followed to prevent or mitigate a loss occurrence. Often, the investigative audit results in a change of policy and procedure to improve efficiency or to raise the level of operational security. This broad area of investigation activity can also be labeled as an investigative audit. If a major loss was uncovered during such an audit, and an arrest affected, it would merely be a by-product of the audit investigation from the organizational point of view. An investigative audit is a major activity of a sound preventive security program.

### *Spot Checks and General Surveillance*

Spot checks of operations and investigative surveillance activities are closely related to audit investigations. These types of investigations are almost endless in nature and limited only by the imagination and resourcefulness of the investigator. Care should be taken that the scope of the activity is coordinated with the internal auditors, even though security spot-checks

procedures in areas that are not considered within the general scope of internal auditing. An example of this type of activity is to conduct unannounced checks on incoming shipments of goods and supplies. One security investigator decided to check a fuel oil delivery being made to the facility. He discovered that the load was short by more than 200 gallons, and subsequent investigation revealed that the driver had been making short deliveries for some time. Because no one had ever checked the metering device to see that it registered zero before unloading, the driver was free to unload some of the fuel before he arrived at the facility.

A surveillance investigation is usually initiated as a result of information received, or it may be just an investigative “fishing expedition.” One hospital security department plants purses or wallets in trousers in high-loss areas. The wallet inside the purse or trousers is attached to a magnetic contact/transmitter. A signal is transmitted to an FM radio receiver when the contact is broken. Another method is to use a light-sensing device to activate the transmitter. This device is particularly useful in moneyboxes, desk drawers, and file cabinets. General surveillance of critical areas can also produce results. Although no losses had been reported in the facility, one investigator set up a surveillance of a general storeroom and discovered that an employee was helping himself to supplies after hours with a key that was not known to be in existence. Loading docks and trash collection areas are also good places for the general surveillance investigation. Alarms and closed-circuit television systems have generally taken the place of the need for staffed surveillance, unless an apprehension is a likely possibility, or the need to intercede in situations where interdiction may be necessary to prevent injury or significant loss of property.

#### *Unemployment and Worker's Compensation Investigations*

There is a great need for the investigation of fraud in unemployment benefits and worker's compensation. Healthcare organizations should become more involved in these areas as government administration and controls are largely ineffective. The proven cases of unemployment fraud may amount to less than 1% of actual cases. These frauds have cost organizations, and ultimately the patient, billions and billions of dollars. The cost of fraudulent worker's compensation claims is many times that of fraudulent unemployment claims. In the worker's compensation claim, not only do employees receive their wages, but there are also physician charges and other unnecessary medical care treatment costs.

## Investigator Attributes

Good investigators have a firm understanding of human relations, a natural aptitude for inquiry, and are intrigued by the investigative process. Investigations always offer a challenge and often succeed or fail in direct relation to the investigator's competence and enthusiasm. A good investigator must have traits as outlined in Table 16-1.

It is generally accepted by the security industry that all investigations are limited by the investigator's reasoning ability. One of the greatest threats to reasoning ability is a lack of objectivity. The excessive influence of subjective feelings, prejudices, or interpretations also severely affects reasoning. Although it is not possible to be 100% objective, professional

**Table 16-1** Desirable Traits of a Successful Investigator

- The ability to remain objective
- Energy and alertness
- Knowledge of the law
- The ability to set realistic objectives
- A methodical nature
- Knowledge of human nature
- Observation and deduction skills
- The ability to maintain meaningful notes
- The ability to interview and interrogate

investigators are able to exert the necessary control over subjective influences to understand any effect they may have on the investigation. The investigative process must be considered to be a major element of the successful protection program. The investigations of many current healthcare security programs need to be upgraded. Administrators and investigators should remember that an investigator is called on to determine the facts and not necessarily to solve the problem. Investigators must at all times conduct investigations within the guidelines set out by the law, and they must always exercise proper employee relations' procedures and conduct. The investigation must be conducted to avoid:

- Compromising a criminal case
- Compromising an arbitration
- Creating a damage action
- Violating the law

In respect to violating the law, the areas of entrapment, invasion of privacy, eavesdropping, and self-incrimination deserve careful attention. Legal actions against investigators and the organizations they represent is always a situation to be avoided.

## Interviewing and Interrogation

In most investigations, it is the interviewing process that consumes over 90% of the total investigative effort, and often the incident or situation is successfully resolved through the interview process alone. Interviewing is intended to gather basic information, facts, and background for leads to further exploration. The interview involves victims, caregivers, witnesses, and others who may have information bearing on the incident being investigated. The interview also has a purpose to obtain information relative to policy, procedures, protocols, and processes that may lead to more in-depth follow-up as the investigation continues. An interview should be conducted in a friendly, businesslike tone and should certainly not be adversarial or overly aggressive. It is simply a matter of asking questions of willing subjects in order to obtain information.

The process of interrogation enters into a relationship with the subject that has sometimes been referred to in initial stages as “adversarial interviewing.” An interrogation,

unlike the interview, is designed to elicit information from a subject who is a prime suspect or a party that knows pertinent facts and does not wish to disclose the information for a variety of reasons. It is the uncooperative nature of the subject that distinguishes the interrogation from the interview.<sup>5</sup>

## Undercover (Covert) Investigations

Undercover operations are widely used in the healthcare setting. The most common activity is to infiltrate an area where a specific or suspected problem exists. The concept of utilizing an undercover operative or concealed security equipment in a patient care facility may seem extreme to some and somewhat frightening to others, but professional security administrators consider it a good business procedure.

### IAHSS HEALTHCARE BASIC SECURITY GUIDELINE, #04.02

#### **Covert Investigations**

**STATEMENT:** Healthcare facilities (HCFs) may require the use of covert investigations to identify persons or gather details about prohibited or illegal acts that occur on the property. Covert investigations may include the use of undercover operatives or electronic equipment.

#### **INTENT:**

- a. Justification for implementing covert investigations may vary greatly (asset protection, drug diversion, rule violations, etc.). The purpose of these investigations will be to collect information to be used as evidence to identify those involved and terminate prohibited activities posing a risk to the facility.
- b. The decision to implement covert investigative techniques should not be made until it is determined that more conventional methods would not be available or would not be effective.
- c. Use of covert investigative equipment (such as hidden or disguised CCTV or other video/ audio equipment) or other covert techniques must be conducted in compliance with applicable local, state, or federal laws.
- d. Consideration must be given as to whether the parties that enter an area under covert observation enjoy a reasonable expectation of privacy. Certain areas in an HCF (restrooms, locker rooms, changing areas, patient treatment areas, etc.) may be considered off limits in regard to covert investigative equipment.
- e. Prior to installing any covert investigative equipment, the security practitioner should determine that:
  1. The activity being investigated has a reasonable chance of being detected.
  2. There is a safe means of installing and removing such equipment (i.e., firewalls are not compromised and other fire detection/suppression/life-safety equipment is not affected in any way).



3. The investigative equipment is concealed so that all such equipment will likely remain undiscovered for the duration of the investigation.
  4. There is a means of retrieving stored information from such equipment without others becoming aware of its presence.
- f. The HCF should develop a policy for the implementation of covert investigations including the following:
1. Designated individuals that can approve such investigations/installations;
  2. Requiring participants to agree to not disclose the investigation;
  3. Evidence obtained during a covert investigation will be considered property of the HCF until such time that it is turned over to a law enforcement agency or other designated recipient. Such evidence will be considered confidential and will not be viewed, disseminated, or discussed with any individuals, departments, or agencies without proper approval;
  4. Finding regarding the investigation and recommendations will be documented and forwarded as appropriate.

**Approved:** April 2008

The covert investigation is intended to protect trustworthy and faithful employees and to ferret out those who are detrimental to the organization. The undercover operation may in deed seem extreme; however, so are the stakes and the responsibility to properly manage the healthcare organization. A successful undercover investigation requires that as few people as possible in the organization know about the operation. Department heads and supervisors generally should not be involved in the plan or privileged with the information that an operative or surveillance equipment has been placed in their department. In a few cases, it may be essential that the department head be part of the effort in order to obtain an open and proper position for the operative, special circumstances, or the type of information being sought. More often than not, however, information leaks begin with the department head and result in a wasted effort and a negative impact on organization staff. A major objective of a covert operation is to severely limit the number of people who know about the operation. The failure to comply with this simple concept has compromised more operations than any other single factor. Generally, if more than two people in the organization, other than the security director, know about the investigation, it should not be initiated, and if it is already underway, serious consideration should be given to aborting the project. In addition to specific investigations, undercover operatives are used as a check on operations to determine whether security policies and procedures are meeting their objectives. It is a method to determine whether the funds spent for security are providing the desired results. Information derived from the investigation need not be negative. Operatives who find that all is going well produce positive and valuable management feedback. After operatives have done their job in one department, they can transfer to another department to continue the audit operation.

Department transfers are sometimes easier to effect than bringing the operative into the organization as a newly hired employee. When an organization commits itself to an undercover program, it must be prepared to fund the program for a considerable period of time. Many undercover programs fail because results were expected too soon. This is especially true of operatives working on a significant problem where those involved are extremely cautious. New people are always treated with a certain amount of suspicion, and operatives must slowly build positive relationships with fellow employees. Of course, the skill and competence of the investigator play a significant part in how much time is required. In large organizations, newly hired security personnel are a possible source of undercover operatives. There are, however, two basic disadvantages to this approach. No matter how thorough the background check and the selection process, the abilities of new employees are always unknown. Another drawback is that not everyone is suited for undercover investigation activities. The wrong operative may produce not only an ineffective investigation, but also cause embarrassing problems for the organization. Another source of undercover personnel is the loan of an officer or investigator from another security healthcare organization. The mutual aid approach can be economical, and the abilities of the personnel are not as unpredictable as may be the case of a newly hired employee. Borrowed and newly hired operatives can do a good job because they have more at stake than do operatives provided by a firm from the outside that will move the operative to other unrelated assignments at another organization. The new hire is seeking a good employment beginning, as well as continued employment. The employee on loan seeks positive feedback on his undercover work to reach his current employer. Undercover operatives should be required to report their activities and observations periodically. This communication should take place at a location outside the organization and is best accomplished in face-to-face debriefing meetings rather than over the telephone. Daily logs of all activity should also be required. Information collected by the operative should be broad in nature and should include any information that might help improve organizational management. To be more specific, information on morale, how well a new policy was received, the falsification of time records, cleanliness, and other items that will help the organization be more efficient should be included in the feedback information. Reports should also include positive information on which systems are functioning effectively.

## Employee Informants

A corollary to the undercover operation is the development of employee informants within the organization. Employee informants are developed in a number of ways. Certain employees naturally develop a good rapport with security during routine contacts. Employees may report possible wrongdoing owing to loyalty or moral motivations. Generally, employees provide just enough information to indicate a problem because they are hesitant to get too involved. These people can often be drawn into an ongoing and productive reporting system. Informants must satisfy a material or psychological

need. The most common motivation is financial. Information is sometimes provided in return for a payment. These payments should always be made when information is received, and the amount of the payment should be based on the value of the information. In the early stages of developing a source, payments may be withheld until the information can be verified. Informants should not receive retainers or regular payments. Another method of obtaining information about employees from other employees is to establish telephone hotlines. These systems provide a means for employees to report wrongdoing while maintaining their anonymity. Various national companies offer this service. The service includes providing materials and presentations to employees on how the system works and the employee's responsibility to report wrongdoing. Organizations using these systems report good success. However, verification of information before taking action is critical because the use of payments can sometimes induce fraudulent reporting.

## References

1. Clark, C. (2009, May 20). 13 hospitals fined for mishaps, never events. Retrieved May 20, 2009, from [http://www.healthleadersmedia.com/content/233406/topic/WS\\_HLM2\\_QUA/13-Hospitals](http://www.healthleadersmedia.com/content/233406/topic/WS_HLM2_QUA/13-Hospitals).
2. ASIS gets legislative win for workplace violence investigations. (2004, January). *Access Control & Security Systems*, 14.
3. Wilson, O. W. (1963). *Police administration*. Location: McGraw-Hill Book Club 282.
4. Blevins, J. Addicts in healthcare professions flock to get peers' help. *Denver Post*, 7/23/09, p. 1A.
5. McDonough, E. (2005). Asking the hard questions. *Security Management*, 88.

# Physical Security Safeguards

In today's world there is an ever-increasing need to improve and strengthen the level of security in healthcare facilities across the globe. As security staff costs are at all-time high levels and physical security advancing technology continues at a fast pace, it is only logical that physical security has been a major source of program improvement over the past decade. While the basic physical security safeguards are still staples of security (barriers/fences, alarms, lighting, lock and keys), it is the electronic components of security that are experiencing explosive growth. In this chapter, the nonelectronic safeguards are discussed, followed by *Chapter 18, Electronic Security System Integration*, which is devoted entirely to the components and implementation of electronic security safeguards.

## Basics of Physical Security

The basic definition of *physical security* applies equally as well to nonelectronic and electronic physical security measures. Physical security can be defined as that part of security designed to protect people; to mitigate the unauthorized access to equipment, facilities, material, and documents; and to reasonably safeguard them against espionage, sabotage, damage, theft, and loss. In most healthcare security systems, the physical security safeguards utilized are intended to be integrated with other components of the security program. In most cases, the physical security safeguards are not intended to function as a stand-alone element of the protection program. For example, security personnel are generally required to inspect, monitor, and respond to the various physical security components of the security system. There is also the interrelationship of physical security and psychological aspects of security that blend together to produce the intended results of protecting patients, visitors, and staff. A good example of this interplay is security signage. Security signage is physical and generally intended to be informational. Signs such as "emergency exit only" or "authorized entry only" do not in themselves prevent exiting or entering. Signs do, however, provide a certain visual aspect of implied control and serve as a notice. This notice puts staff in a position to ask a stranger of their purpose in a restricted area and may prove useful in criminal trespass or other type of action.

## Designing a System of Perimeters

The securing of a healthcare facility is often described as a system of perimeters in which each succeeding perimeter is closer to the most critical areas or operational functions of the facility than the preceding one. The term *security layering* is somewhat confused with the term *system of perimeters*. Security layering simply means using several different security safeguards to provide the level of protection desired for a given area, or the security risk(s) being addressed. For example, a parking lot may be protected by video surveillance, fencing, signage, emergency communication devices, lighting, and patrolling security officers. Each of these safeguards would be considered a “layer,” or in a simple sense the recipe of security elements deployed as the protection package. The facility grounds, including the parking areas, are the first perimeter for security consideration because the natural environment rarely provides adequate security; in fact, the environment can create additional security needs. [Figure 17-1](#) illustrates the concept of security as a system of perimeters.

Some older healthcare facilities have extensive brick, stone, or concrete walls enclosing the facility. These barriers, which were generally patterned after European facilities, were probably built more to provide privacy than to provide protection. The cost of construction today has practically eliminated the wall as a form of protection. The outer building walls of modern facilities are often the first line of perimeter protection in urban areas, where many building walls are indeed the sidewalks and property lines. As new facilities have been built in suburban areas, there are spacious grounds that create a campus environment. Some level of security is generally implemented at the outermost perimeter line to serve the various functions of deterrence, delay, detection, access discrimination, and boundary identification.

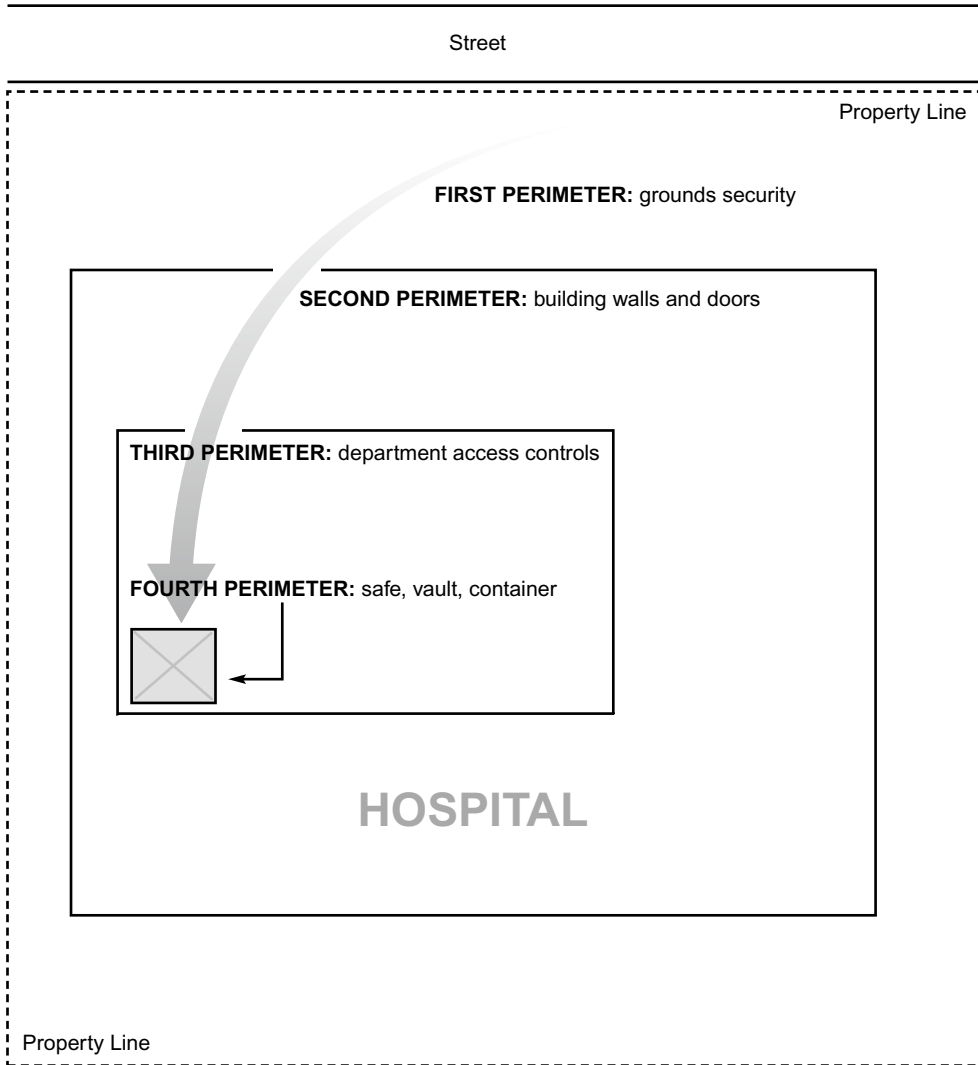
## Barriers

Barriers are one of the oldest forms of physical security and are either manmade or natural. In the early days of settling America the covered wagons were formed in a circle at night. In the era of castles the moat provided a barrier to protect the castle. Rivers and steep terrain have always served as natural barriers and still serve as an element of protection to a limited degree today. In short, a physical security barrier is an obstacle to the movement of persons, and in some cases animals, especially in rural and urban areas. In the recent past, video images of a moose entering through a door into a medical clinic were widely circulated among healthcare security practitioners.

Our discussion in this chapter will focus on the common manmade barriers currently being used in healthcare security programs.

## Fencing

Fencing as a barrier is one of the oldest forms of physical security. Although it is a meaningful protection element for many facilities, it may not be a practical application of



**FIGURE 17-1** Security viewed as a system of perimeters.

control for specific situations. The proper application of fencing as a safeguard is largely dependent on the layout and design of buildings and grounds, and organizational philosophy in terms of aesthetics and the image portrayed. The term *fencing* can send some healthcare administrators over the edge. They are just simply opposed to fencing. Not all fencing is the same and the use of different types of fencing barriers can actually enhance the image of the facility. Fencing need not always completely surround an area. It can be effectively used to control traffic patterns and to define property lines for only certain areas or parts of the complex. A fence might imply to the community that the facility is

sealing itself off from its neighbors. For this reason, if fencing is required, facilities should consider installing it in segments to minimize its perceived negative impact. Fencing can be ugly, or it can be somewhat pleasing. Fencing is generally installed (or considered) in healthcare facilities as a result of various protection problems that arise; it is rarely part of the original design. The exceptions are government and private facilities with large amounts of land; in these cases, fencing is often planned in the design stage. Fencing a large tract of land usually produces no adverse effect on public or community relations.

Surface parking areas are prime locations for protective fencing. The basic premise behind fencing parking areas is that criminals generally do not want to engage in their criminal activity where the means of escape is limited. On the other hand, fencing may limit a victim's escape route. General experience, however, demonstrates that properly fenced areas are considerably safer than unfenced areas.

### *Chain Link Fencing*

The basic type of fencing used in the security industry is the galvanized steel, chain link fence, which permits visibility from both sides. The protection offered by this fencing is directly proportional to its height. A short fence is basically a psychological barrier, but a high fence with barbed-wire outriggers or a razor-ribbon topping is a physical security barrier. When barbed wire and other types of toppings are offensive to members of the healthcare organization, increased height is a good alternative. If an area requires fencing, the minimum height of the fence should be 7 feet for security purposes. Barbed-wire support arms (outriggers), if required, should be placed at a 45° angle to the upright posts. The arm should face toward the direction that penetration is to be denied. In the healthcare setting, situations rarely require support arms on both sides. Additional protection can be gained by burying the bottom of the fence below grade to minimize digging under the fence to allow a person to crawl under it. Fencing has many applications in healthcare facilities in addition to parking areas and property lines. Among the most common enclosures are oxygen storage, chiller towers, water retention ponds, gasoline or fuel dispensers, outdoor equipment storage, and bicycle storage areas. [Figure 17-2](#) is an example of utilizing fencing to provide a barrier between buildings, with the objective of being an access control measure.

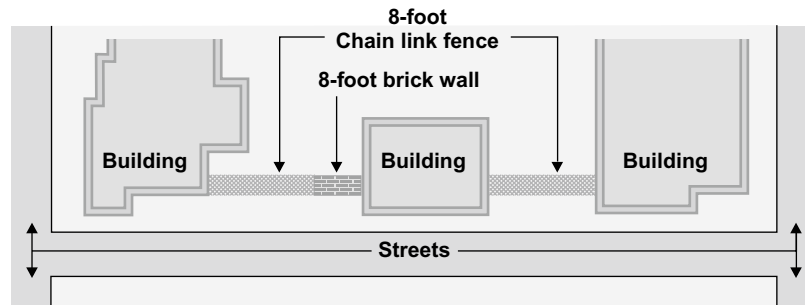
The mini-mesh chain link fencing material is recommended where a greater level of protection is required than that afforded by standard chain link fencing. The mini-mesh wires are thicker and the mesh is much tighter. This type of chain link fence provides good breakthrough strength. The closer mesh does not offer easy hand- or foot-holds and the mesh spaces are small enough to resist the use of bolt cutters. This type of chain link fence is ideal for oxygen storage areas and should be at least 8 feet high to provide the level of protection required. The fencing line base should be concrete or asphalt. If in dirt, the fence should be buried between 12 and 18 inches.

### *Decorative Metal Fencing*

The use of iron or aluminum fencing is gaining in popularity. It is more expensive than the standard chain link fence and thus used where there are fairly short runs and aesthetics is

a priority. This type of fence is sometimes referred to as wrought iron, but comes in a variety of round, square, and rectangular material. These fences have good see-through visibility and breakthrough strength can be quite high, as the fencing material cannot be easily or quickly cut. In many applications this type of fence not only provides security, but also enhances the suitability of space used by patients, visitors, or staff. Figure 17-3 portrays the use of a decorative iron fence surrounding a hospital outdoor garden that provides security while actually enhancing the aesthetics and a feeling of comfortable and inviting space.

The stark appearance of fencing can be minimized with landscaping. However, the landscaping design must exclude any heavy foliage or shrubs, which can provide a hiding place for contraband, vagrants, and intruders. Thorny foliage may serve as an effective barrier by itself or in combination with fencing.



**FIGURE 17-2** Example of the use of fencing and brick wall for security.



**FIGURE 17-3** Example of a decorative iron fence providing a pleasing definition and security for an outside garden area. (Courtesy of The Children's Hospital, Aurora, Colorado).



## Bollards

A bollard is a short vertical post that is increasingly common around the world to hinder vehicles from achieving close proximity to buildings or critical elements of the facility infrastructure. The use of such devices has grown since the increase of terrorist bombings and the incidents of ram-raiding. Ram-raiding refers to the criminal activity of ramming a store/building for the purposes of burglary and theft.

The bollard is being employed by healthcare facilities to prevent the intended, or unintended, ramming of a vehicle into vulnerable areas of a building. The common locations of such vulnerability are glassed door entry areas off driveways and ramp areas. The most notable areas at risk would be the Emergency Department Ambulatory and the Emergency Medical Service (EMS) or ambulance entry points. The bollard is also used to prevent damage to utility connections such as a gas meter, electrical stations, oxygen storage tanks, and such. They are also widely used in parking areas and structures to control traffic, prevent damage, and provide an element of safety for persons using the parking facilities. Not strictly a physical security safeguard, a hospital in Stockton, CA, installed protective bollards outside of their emergency services entry after a visitor accidentally drove his truck more than 10 feet into the glass entrance.

The design of the bollard and its installation is largely determined by the security risk that is being managed. A bollard placed in the middle of a wide walkway to prevent use by motorized vehicles would be of a more lightweight construction than the bollard intended to keep a vehicle from crashing into an entranceway. The common bollard is steel pipe of varying circumferences filled with concrete. The steel pipe is then anchored in concrete at an appropriate depth as a fixed solid bollard. Some bollards can be removed to allow temporary access. A common design for this type of bollard is to lock it in place after lowering it into a slightly larger size pipe and locking it in place.

## Lighting

Security professionals generally agree that exterior lighting is one of the most basic and cost-effective components of the protection program. Exterior lighting serves two distinct purposes: safety and security. Safety lighting provides the means for persons to navigate the exterior, avoiding slips, falls, and environmental obstacles. Security lighting, on the other hand, is designed to discourage criminal activity and to provide light for surveillance purposes. It is important to note, however, that lighting also creates a feeling of safety and can thus conceivably create a false sense of security.

### Selection and Design of Grounds Lighting

When selecting and installing external lighting, the security administrator must consider the potential for vandalism of the light fixtures. The proper design and location of the lighting fixtures reduce the probability of malicious destruction. One method is to install light fixtures as far inside the property line as possible (facing outward) and to use

**Table 17-1** Lighting Characteristics<sup>1</sup>

Lighting Characteristics		
Type	Lumens Per Watt	Color Discrimination
Incandescent	20	Excellent
Mercury vapor	63	Good
Fluorescent	83	Excellent
Metal halide	115	Excellent
Sodium	130	Fair
Light-emitting diode (LED)	131	Excellent

break-resistant cover guards. Lighting fixtures should also be designed so that the failure of a single lamp will not create an area with reduced protection or reduce the light below acceptable standards. [Table 17-1](#) lists the six most common types of lamps used in security applications.

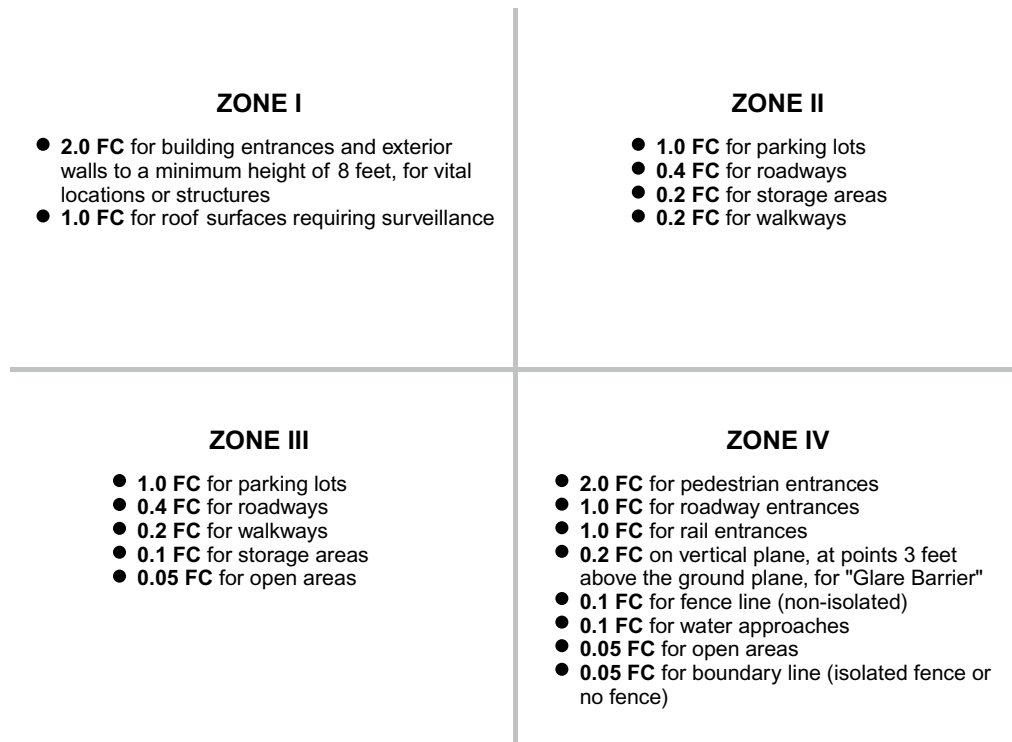
The quality of exterior lighting is often reduced by tree foliage. Pruning the foliage or altering the position of the lighting fixture may correct this problem. Security personnel should ensure that lighting operates at maximum effectiveness by regularly checking for encroaching foliage and reporting any lights that have burned out. The amount of night lighting required varies according to the area's crime vulnerability and the security administrator's judgment, based on the security risk assessment. More light is required at entryways and walkways than is needed in most parking lots. [Figure 17-4](#) shows the lighting requirements that are considered to be a standard of the security industry.

## Trees and Shrubs

Trees and shrubs can be used to create physical barriers or to enhance other barriers to increase security protection. On the other hand, trees and shrubs may provide a convenient hiding place, a place to dispose of or hide contraband, and a place to store stolen property for later retrieval. The use of shrubs that have substantial thorns might mitigate the shrub being used for concealment. Landscaping need not be sacrificed for security purposes; rather, the landscaping should be planned and maintained to meet security objectives. The word *maintained* is important. A small shrub that does not present a security hazard when planted can grow into a problem in a relatively short time. When new landscape architectural plans are developed, the security administrator should require the plans to be superimposed over the exterior lighting plan and reviewed over a 1-year, 5-year, and 10-year horizon. Often, landscape design is focused on providing more immediate beautification to enhance the image of the opening of a new building or provide initial assistance with erosion control. Too frequently, landscape architects fail to consider or discuss how the expected plantings may impact security lighting. The security

## SECURITY NIGHT LIGHTING STANDARDS

Lighting standards are grouped into the following zones.



**FIGURE 17-4** Commonly used standard for security lighting (Source: *IES Lighting Handbook*, 5th Edition, and American National Standard Practice for Protective Lighting. Published by the Illuminating Engineering Society, 345 East 47th Street, New York, NY, 10017).

administrator will find the organization much more amenable to moving a tree during the design stage than requesting the removal of a tree once it is fully grown.

## Locks and Keys

Locking devices of all kinds are a primary element in virtually all security systems. Electronic locking systems are rapidly replacing the traditional lock and key systems for many areas of a facility. Electronic access control systems are more fully discussed in *Chapter 18, Electronic Security System Integration*. However, there will always be the

need for the traditional key applications. It is estimated that misplaced keys cost organizations in North America approximately \$35 billion annually in terms of inefficiency, shrinkage, liability, and lock replacement costs.<sup>2</sup> Locks come in all sizes and shapes, and they function in a wide variety of ways. In most applications, the lock is intended to serve two basic purposes. The first is to delay a compromise of the security system. Different locks will delay compromise for different lengths of time, and the selection of the lock should be based on the protection level required. A sturdy lock will discourage an amateur and will force a professional to work harder to compromise the locking system. The second function of the lock is to provide visual evidence that the lock was compromised when such compromise occurs as the result of physical force. The level of protection a lock is designed to provide against someone who does not possess a key, a combination, or other information is fairly easy to calculate. The protection level drops significantly, however, when the lock and key program is poorly administered. The initial risk is that an unauthorized individual will *obtain* a device or information to operate the locking mechanism. The second risk is the *unauthorized use* of the device or information by an individual who has obtained it. In both cases, a false sense of security prevails because an intruder can gain entry for unauthorized purposes without leaving evidence that the system has been compromised. Locks used in conjunction with alarms or recording devices are necessary in preventing and detecting both break-ins and unauthorized use.

## Administering the Lock System

It is an unfortunate fact that the lock and key systems in over 90% of healthcare facilities are inadequate. This widespread inadequacy is more often the result of lax administrative controls rather than improper hardware. However, the improper use of hardware, which either defeats the purpose of the lock or fails to provide the protection level assumed, contributes to the problem. Facilities spend large sums of money on locking hardware, but many fail to provide the funding and administrative control required to properly manage the system. In any healthcare facility of at least 300 beds, a security administrator who is given full responsibility for the lock and key program can reduce the number of required locks, lock changes, and keys issued to such a degree that the money saved will be enough to pay for the personnel required to properly administer the program. It is generally recommended that the security department administer the lock and key control system. Just as checks and balances are required in cash accounting, with one individual performing a certain step and another individual performing another step, the principle of separation of responsibilities applies to key control. The person who controls the key-cutting equipment (often someone in the maintenance department) should not control the key blanks. The authorization for keys and the key blanks required should be forwarded to the person who will actually perform the work. An effective system might work along the following lines: The security representative receives a request for a key, a lock change, or a new lock. After establishing the validity of the request, the security person forwards a work order (perhaps the original request form) to the person or department that will perform the work. The key

is then returned to the security department for issue. In some large systems, the locksmith function may actually be part of the security department. This is a good arrangement, but in most facilities there is not enough work to keep an employee busy with this responsibility. It is not uncommon, even in some large facilities, to contract out all lock and key work to a local locksmith. If this is the case, the control system should still remain the specific responsibility of a facility individual or department. A key may be issued to an individual, or a group of keys may be issued to a section or a department. Individual key issue by the security department is the preferred method. This system provides a central record, and the status of the system can be accurately assessed at any time. This method of security department control requires a rigid system of procedures to ensure that terminating employees are routed through the key control center. A substantial key deposit should be required as an incentive for individuals to return keys, even if the key is returned by mail or by other means if they do not go through the regular termination process. Deposits of \$25 to \$50, which tend to render the key control program effective, may be necessary. Fragmented key control may be unavoidable due to the distance between facilities or the failure of the administration to recognize the value and cost/benefit of a centralized key issue system. In the fragmented approach, the security department still remains responsible for authorizing lock and key work. The difference is that the keys are released to sections or departments rather than to individuals. The departments then have the responsibility for issuing the keys, maintaining the records, and retrieving the keys before or during the employee termination process. A point in favor of the fragmented system is key retrieval. Individual departments are the first to know of terminations for cause and voluntary resignations; this knowledge should enhance key retrieval. However, proper records must be maintained to determine the number of keys that have been issued to each individual.

### Interchangeable Core Locks

The convertible or interchangeable core lock design is a feature of pin tumbler locks that provides a rapid and simple redistribution of combinations. It can be replaced at the lock location by another core already configured to the system. Interchangeable cores save labor time and a reduced technical skill level is required to make single or large-scale lock changes. It takes 30 to 45 minutes for the average healthcare locksmith to change the combination of a conventional pin tumbler lockset. By contrast, the interchangeable core lock takes between 5 and 10 seconds to remove one core and insert another. Although the initial cost of the changeable core system is somewhat higher, the efficiencies gained with the system more than offset the difference in cost. If one truly wants to save money on his/her locking hardware, the place to begin is to reduce the number of locked doors—doors that did not need a lock in the first place.

### Master Key Systems

An important decision that must be made when designing a lock and key system concerns master keying. A master key system is generally divided into four levels: (1) the

change key, (2) sub-master, (3) master, and (4) grand master. Many security professionals are reconsidering the actual need for and the limitations of the master key system. Master key systems require a considerable investment in hardware and labor, and often the master key becomes a status symbol rather than an effective security safeguard. Master key systems actually reduce the security capability of a lock by providing fewer usable combinations. Master keying is generally a matter of convenience rather than a security safeguard. When planning a master key system, a growth rate of 300% over 10 years should be assumed to avoid prematurely outgrowing the system. A total of 10–12 years should be regarded as the practical limit of the system. The obvious disadvantage to the master key system is the complete compromise of the system when the master key is lost or when unauthorized duplicates are produced. A typical progression in a master-keyed complex is to remove an increasing number of locks from the master key system as the result of security problems that indicate that the master key may have been used. Certain locks should not be placed on the master key system. The number of exceptions depends in large part on the number of master keys distributed. Examples include certain pharmacy areas, some storerooms, and perimeter doors that should be controlled by an electronic access system. Many security administrators cling to the concept that security officers must carry a master key in the case of emergency. This view is not necessarily valid. In numerous facilities that are not master-keyed, the security function is still accomplished. Security officers should have the means to obtain timely access, on a controlled basis, to any part of the complex, but neither a master key nor requirement to carry a big ring of keys is an absolute necessity.

### Computer-Based Key Accountability

Traditional methods of key control are paper records of key issue dates, to whom issued, lost keys, and a log entry when the key is returned. This method is labor-intensive, prone to error, and it is difficult to track down a specific key issued or to analyze a pattern of key usage. This obsolete and ineffective method of key control has largely been replaced with key management systems that provide computer-based key tracking. Most of these systems involve a locked key cabinet with numerous types of access control, such as key pads, biometrics, proximity or magstripe cards, all available to be integrated into an advanced key management system. In these advanced systems, each key is locked into place using a key with an integrated chip that allows only the removal of a key by an individual for whom authorization has been issued. It is common that the system lights up the location for the key or keys the user can remove. The cabinets can be grouped together to increase storage volume or can be in multiple locations controlled from a single personal computer interface. Cabinets are not only for keys, but can also be used as lockers to store firearms, radios, hand-held computers, and like items. These systems can be programmed to allow the release of a specific key(s) that the individual is allowed to check out down to specific time periods, including an alarm condition if the key(s) have not been returned within a predetermined time period. Management reports can be generated that list the

keys that have been issued to an individual, including the time issued and the duration of time before return of the key(s). A printed audit trail of a specific user or of specific key(s) can be easily generated.<sup>3</sup>

## Lock Installation

No type of locking mechanism is totally effective unless it is installed correctly. All too often a facility spends a large sum of money to buy the proper lock but fails to install it properly, resulting in a degree of protection no better than a less expensive and less suitable lock would have provided. A common problem encountered in lock installation is that the bolt does not penetrate (throw of the bolt) the doorframe sufficiently. The throw should be a minimum of 1 inch. If there is a wide space or a gap between the edge of the door and the doorframe, the bolt throw may have to be longer. The door and the frame must be substantial enough to resist physical attack. If they are of doubtful strength, it would be uneconomical to install an extremely resistive locking device. The weakest part of all the components determines the resulting level of protection being provided.

## Lock Changes

No matter what, keys will be lost and unaccounted for over a relatively short period of time. It is, thus, a matter of judgment when a certain lock should be changed. This decision generally takes into consideration the number of lost keys for a particular lock, how critical the area protected by the lock is, and what additional layered safeguards are used in protecting the area. All organizations should have a schedule of changing locks as an ongoing program. It is usually possible to obtain capital equipment funds when budgeted as an ongoing replacement and improvement project as opposed to a large amount at one time. The schedule should be developed so that the locks in each area of the facility are changed every 5–7 years. The ongoing program avoids a high cost all at one time, permits higher priority areas to be selected, and makes a key system control much more manageable.

## Push button Locks

Electrical and mechanical push button locks have gained popularity over the past 10 years. These locks are particularly advantageous where a large number of people require access. The major advantage is the ability to change the lock combination instantly without incurring the cost of changing the lock and reissuing keys. Common areas of use in healthcare facilities are nursing and doctor lounges, small storage rooms, and restricted areas. These locks can be quite simple and inexpensive, with single combinations, or they can be high-security locks that require a push button combination and an access card. Some electronic locks require no wiring and permit hundreds of combinations and time schedules. Another advantage of push button locks is that authorized personnel need never be locked out. There is no key to lose and no access card to leave in another coat or purse.

## Padlocks

When planning lock systems and security controls, padlocks should not be overlooked. In areas where aesthetics are not important, a casehardened padlock can provide a high level of protection at a reasonable cost. As with door hardware, proper installation of the hasp is paramount. Security departments should maintain several padlocks for temporary use. One security department paints a red stripe around the body of its padlocks to give an instant visual message that the padlock is a security department controlled lock. A plastic tag, which moves freely on the shackle, clearly identifies the lock as a security padlock and states that the central security control desk must be called to open the lock.

## Key Making

There are various preliminary steps to establishing a key control program. First, each lock location must be identified. For door locks, each room must be numbered or identified, and any doors within these rooms likewise must be identified. The number or other reference given to each door need not appear at the actual location and can be identified on a lock control drawing. However, the doors or rooms should be numbered at their location as a means of identifying these areas for other purposes, such as maintenance work orders, deliveries, and visitor information. All rooms should be identified, regardless of whether the doors currently have locks, because locks may be installed later. Another element of key control is marking or identifying the keys themselves. For obvious reasons, keys should not be marked with the specific lock number or room number to which the key belongs. Numerous codes have been devised by specific organizations to fit their purpose. It is suggested that letters of the alphabet be substituted for numerals, either selected randomly or through 10-letter code words. The latter system is advantageous when many individuals need access to the code, because the code need not be written down. Written codes are subject to a greater degree of possible compromise. Keys fitting multiple locks require additional code markings, and the method used for cross-referencing is based on the security administrator preference. Consideration should also be given to marking keys with the words *DO NOT DUPLICATE*. The effectiveness of this practice is unknown. Many places that provide key-cutting services ignore this stamp; however, many professional locksmiths will honor it. Furthermore, this marking may deter employees who want a key, but are reluctant to try to have the key duplicated. Locks from numerous manufacturers can be ordered with key blanks that are not generally available except to the organization that purchased the lock. Security is further enhanced when keys must be cut at the factory to fit a particular lock. One lock manufacturer provides a lock with one set of keys, and beyond this original set no keys may be duplicated. The keys are marked to identify each key and the total number of keys in the set. For example, a set of three keys would be marked *1 of 3*, *2 of 3*, and *3 of 3*. This type of lock obviously enhances security, but can be expensive if staff does not exercise extreme care in the accountability of the keys.



## Periodic Inventory

Regardless of whether the key distribution system is centralized (keys are given directly to individuals) or decentralized (keys are given to departments, which pass them out), a procedure must be established for periodically inventorying the keys in the possession of individuals. This responsibility should be assigned to the security department. In the decentralized system the security department must first check the records of the various departments to determine whether all keys issued from the security department can be accounted for. The next step is to contact each employee who has been issued a key and to check the existence of the key. The security officer must also see each key in the central system. Various methods can be instituted to make this an ongoing program. The processing of identification badges and the inventorying of keys can occur simultaneously. In one system, identification badges expire on the employee's anniversary of hire. When employees are processed for new badges, the security department checks the records to determine whether they have been issued any keys. If so, the keys must be accounted for before the new badge is released.

## Seals

In the absence of an alarm system, a wire, a metal band, or a plastic seal may be used to aid in determining whether an area has been entered. These seals also help to discourage unauthorized entry. The system is simple but effective. The security officer applies a seal on the doors to an area after all access requirements are over for the day. Examples of areas that might be sealed include the main storeroom, gift shop storage area, laundry, library, electronic data processing department, and maintenance storage area. On each patrol, the security officer can check the seal to determine whether access has been gained. The officer can remove the seal at a preset time or by the first department employee to arrive the next workday. In most cases, the maintenance department will have to install eyelets on the door and the doorjamb to provide a means of looping the seal. Because the seal can be easily broken and thus does not provide any real physical protection, the eyelets need not be overly secure. Extra long seals can be used to loop through fire exit release devices and for similar applications.

## Glazing (Glass)

After doors, the second most common openings into rooms or buildings are windows. Doors with glass are also plentiful and, when regular glass is used, invite easy compromise of the locking device. Although illegal entry is a prime security vulnerability, glass windows and doors with glass windows also present a potentially costly vandalism problem. Another problem associated with windows is vulnerability to an arson attack by means of a Molotov cocktail or a flammable liquid being poured through a broken window.

## Acrylic Plastic

An alternative to using regular glass is acrylic plastic (sometimes called *polycarbonate*) or a glass laminate with an acrylic core. The latter is the most expensive, but it offers the best protection against physical force, blowtorches, and projectiles. Acrylic plastic has the benefit of being lightweight (approximately one-half the weight of glass). Until recently, the greatest problem with the acrylic sheet was its tendency to scratch easily and to lose its transparency from even routine cleaning. Most manufacturers of acrylic sheets now produce a coating product that minimizes deterioration.

Protective screening and decorative ironwork have been used effectively over the years as added protection for glass windows and other openings. This type of protection is often utilized at small freestanding clinics and physician office buildings. The visual effect of bars on windows and openings projects a poor public relations image.

## Bullet Resistive Glass

The term *bulletproof glass* is a misnomer, with the term *bullet resistive glass* being the proper nomenclature. Bullet resistive glass is basically made by layering a polycarbonate material between pieces of ordinary glass in a process called *lamination*. This process creates a glass-like material that is thicker than normal glass, ranging from an approximate thickness of 7–75 mm. Polycarbonate is a tough transparent plastic often known by the brand name of Lexan, Tuffak, or Cyrolon. The ability of bullet resistive glass to stop a bullet is determined by the thickness of the glass. It is interesting to note that there is available a one-way bullet resistive glass that has one side able to stop a bullet, while the other side allows bullets to pass through unaffected. This feature provides the person being shot at the ability to return fire<sup>4</sup>—a feature that probably has little or no application in the protection of healthcare facilities. On the other hand, polycarbonate glazing is frequently used to protect pharmacy transaction windows, cashiers, admissions clerks, glazing in a behavioral health unit, and even in some door applications where breakage (safety) is a specific consideration. When polycarbonate glazing is used, other physical safeguards surrounding the area to be protected should not be forgotten. Specifically the walls under, over, and around the protected area should be reinforced with metal or other strong material to fully institute a protected compartment.

## Fastening Down Equipment

The familiar saying “They’ll steal anything that isn’t nailed down” is certainly true in health-care facilities. Items that should be “nailed down” include computers, audio-visual equipment, microscopes, and other expensive pieces of equipment. With the many relatively inexpensive locking devices that are commercially available today, there is little excuse for any organization to suffer substantial losses of essential and expensive items. Electronic tagging equipment with sensors that sound an alarm when there is an attempt to remove the equipment from the “protection field” is also becoming increasingly popular. Some

facilities still prefer to bolt down equipment. If this is the case, equipment service representatives should perform this work rather than in-house maintenance personnel. Undue stress on equipment and the use of bolts that are incorrect can result in damage to the equipment. Insurance companies are reluctant to provide incentives for organizations that protect their own property, but it does seem that locking devices would be effective in reducing insurance costs. The high deductibles of most insurance policies, however, translate to hospital out-of-pocket loss rather than to insurance company–paid claims.

## Marking Property

Conspicuously marking organizational property is a cost-effective means of reducing property loss. Asset number tags, although important, do not deter theft to any extent and can generally be easily removed. Marking hospital property serves the following purposes:

- It identifies the ownership of the property in the case of theft.
- It assists with management accountability controls (inventory).
- It provides a visible sign that the property being removed is hospital property.
- It serves as a deterrent to theft.

The wheelchair is a good example of an item that should be marked. Many privately owned wheelchairs are brought into medical facilities every day. When security officers or other staff observe a wheelchair being folded up and placed in a vehicle, they must be able to determine whether the wheelchair belongs to the organization. How should a wheelchair be marked? First, the fabric should be a special color, ideally one that is not popular for private wheelchairs. Next, the back of the fabric should have the organizational logo or initials stenciled in at least a 10-inch square. The location, department, and wheelchair number may also be useful in the day-to-day use and accountability of the equipment. Finally, small bands should be painted or taped on certain tubular parts of the chair to further distinguish it from personal property.

## Safes

Safes are often the targets of criminals because the mere existence of a safe engenders visions of valuable items. The safe is a formidable looking piece of equipment, but it does not always afford the protection assumed by its owners. Healthcare facilities use safes, or vaults, to protect records, certain drugs, cash, patient valuables, and negotiable paper. Regardless of the item being protected, the best protection is to reduce the quantity of stored materials and examine the storage container to see that it is designed to furnish the protection required. Safes are similar to locks in that a false sense of security can be created when the equipment is misused or misunderstood. Perhaps half of the healthcare professionals who use safes do not know the difference between a safe designed for fire protection and one designed for the storage of cash and valuables.

## Fire Safe

Facility surveys often reveal a record safe being used for valuables. A record safe is designed to protect against fire only. The fire-only safe is generally constructed with wet insulation poured between two very thin steel walls. Water is retained in the insulation, and when a fire occurs, the water creates steam within the safe. The steam acts as a cooling agent and holds the internal temperature below the flash point of paper (350° Fahrenheit). These safes are designed to withstand only one fire; after that, the insulation no longer provides protection. The UL label inside the safe indicates the length of time the safe will provide protection during a fire. The construction of the walls of the record safe is so thin that they offer little protection against forced entry.

## Valuables and Multipurpose Safes

The burglar-resistant safes are constructed of heavy steel plate, and some are reinforced with ceramic or metal filler to increase protection against torches and burning bars. The UL ratings indicate the length of time the safe can withstand attack. Because fire will cause heat to build up inside, burglar-resistant safes should not be used to protect paper records. Multipurpose safes are also available; these are basically fire safes that have an inner protection liner to render it a burglar-resistant safe. Safes should generally be bolted to the floor. It is not uncommon for a safe to completely disappear from the premises—and often the safe is worth more than the contents. Placing the safe so that it can be regularly inspected and providing proper lighting are additional commonsense safeguards. Safes containing high-risk materials may also need the added protection of an alarm system. Several types of alarms are designed specifically for safes. Safes must always be used properly, and there is no substitute for storing as few items as possible.

Many inpatient organizations are placing burglar-resistant safes in patient rooms during new construction or room renovation efforts. Providing a safe to patients during their stay is yet another step to encourage patients to secure their valuables while in the hospital. Organizations that use these safes have experienced a reduction in the loss of patient valuables.

## Signage

Signs and more signs are everywhere. Our environment is overloaded with signs of every kind, shape, and color. Despite the problem of sign proliferation, there are certain signs that are basic to healthcare security programs. Security signage can effectively direct and inform people without the need for “live” security intervention. They can also serve as the foundation to initiate legal action or be a defense against legal action directed at the organization. In some cases, certain security and safety signs may be required by legislation and/or requirements imposed by regulatory agencies. These signs can be viewed in two types: (1) command signs; (2) informational signs. There is of course some overlap and linkages between these two types of signs, and a single sign may be a combination

of the two types of signs. For example, a way-finding sign would be classified as informational; however, it does aid the security objective of reducing the wandering of persons throughout the facility. Reduced wandering aids in less disruption of services and the possible commission of a crime due to the presentation of an opportunity. Both types of signs may be directed at specific groups, such as staff, visitors, and patients, or they may be directed to all persons.

## Command Signs

The command signs tell people what to do or what not to do, such as “No Admittance,” “Authorized Personnel Only,” and “Drug-Free Zone.” The command sign may be direct, with no attempt to make a point with public relations in mind. Another approach to some signs is to use humor to draw attention to expected compliance. An example of the humor approach might be a sign in an Emergency Department waiting area that reads, “Any children left unattended may be held for ransom.”

## Informational Signs

The informational signs provide knowledge to alert people, such as “Emergency Telephone,” “Fire Extinguisher Location,” “Property Protected by Video Surveillance,” “Door Locked at 8:30 A.M.” In terms of good business, and good public relations, it is highly recommended that all entry doors that the public may approach for entry to the facility have informational signage that states either the hours it is open for public use or the hours it is closed to entry. There is some debate as to whether this particular signage should be either time open or time closed. Some hospitals have added wording to direct persons to a night entry point, such as the Emergency Department entrance or other designated night entry points. This type of door information could be rather small lettering at the location a person is reaching to open a door. A small black lettering decal-type sign works well on glass and does portray an uncluttered look.

## Control and Uniform Signage

A major reason healthcare administrators are relatively antisign persons is that there is no organizational policy and procedure relative to the type and permissible placement of signs. As a result, signs are often handmade and taped to a wall. Even permanent signs that may be for the same purpose are often quite different from place to place. It is quite common to visit facilities that may have as many as six or seven different looking (size, shape, color) signs that have the general message of “Emergency Exit Only.” This occurs as some of these signs are implemented at different time periods by different people, almost department by department. Not all security signs are created equally in terms of obtaining voluntary compliance. An “Emergency Exit Only” sign that states an alarm will sound generally has a better compliance percentage than one without. In one hospital that had an emergency exit sign that was being consistently ignored, a change of color

and configuration of the sign to one that resembled a traffic STOP sign reported a 300+% increase in compliance.

A word of caution concerning security signage: Do not be tempted to post signs to fend off criminals or wrongdoers that may not be true or send a message that may be misconstrued. The “Property Monitored by CCTV” sign should not be posted if no equipment is in place, if it is of limited value, or when real-time monitoring does not occur. This signage may create a false sense of security in the context of a person’s perception that they are better protected than is actually the case. An assault in a parking lot or garage could lead to costly litigation if the victim was able to convince a court that the security signage was false or misleading.

## Crime Prevention Through Environmental Design

The basic concept of Crime Prevention Through Environmental Design (CPTED) is that crime can be prevented or mitigated by design of the internal and external environment of a facility to increase crime deterrence and the likelihood of apprehension of criminals. The concept of CPTED began in the early 1970s with such writing as Oscar Newman’s book *Defensible Space*, and later the book of Dr. C. Ray Jeffery entitled *Crime Prevention Through Environmental Design*.<sup>5</sup> The three overlapping strategies of CPTED are (1) natural access control; (2) natural surveillance; and (3) territorial reinforcement. Utilization of these three strategies produces a proactive, unobtrusive perception of safety by visitors, staff, and patients.<sup>6</sup>

### Natural Access Control

Designing access pathways that provide direct access to the intended destination of patients and visitors (and sometimes staff) is intended to reduce criminal or other negative behaviors. An example is the placement of outpatient clinics. The objective of access control would be to have clinic patients and visitors arriving at their destination immediately upon entering the facility and when finished with their business, to depart directly to the outside. This access control plan and space allocation would also involve providing the parking area intended for the clinics to be immediately outside of the clinic ingress/egress point. In short, the clinic should not be located into the interior of the facilities, requiring clinic patients and visitors to walk through or near operational departments or functions.

### Natural Surveillance

Natural surveillance includes the placement of windows and open areas with clear lines of sight. Grounds and parking areas are prime locations to provide clear lines of sight to prevent potential assaults by reducing hiding places or shielding illegal or unwanted behaviors. One hospital that experienced an assault on its grounds immediately reduced bushes and trimmed trees so that no tree branches were less than 7 feet from the ground. Natural surveillance also refers to activities that have a relatively high number of people

in the area for the designated function or activity. The theory is that more people provide a less attractive environment for a negative or criminal act. This theory did not, however, work at one hospital where the cafeteria cashier was robbed at gunpoint at high noon on a Friday with the cafeteria operating at full capacity.

## Territorial Reinforcement

Territorial reinforcement relates to the natural progression from public to private space. Clearly defining the boundaries between public and private areas of the healthcare campus and buildings establishes a sense of ownership. The message conveyed is that the private area is off limits to anything other than the intended use and activity. The idea being presented by this CPTED concept is to increase a person's subliminal perception of an area as being secured or inaccessible.

The actual implementation of CPTED practices is best begun in the planning phase of new space construction, renovation, or function relocation. In most cases, the concepts of CPTED will require various physical security measures to complete the control process.

## References

1. Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to security* (8th ed.). Boston: Butterworth-Heinemann pp. 186–189.
2. McGovern, M. (2008). Who has the keys? *Security Products*, 52.
3. Pires, F. (2009, March 3). Key boxes have come a long way. Retrieved March 12, 2009, from <http://www.campusafetymagazine.com/news/?NewsID=2754>.
4. HowStuffWorks.com. (2000, September 26). How does "bulletproof" glass work? Retrieved June 8, 2009, from <http://science.howstuffworks.com/question476.htm>.
5. Ahrens, S. A. (2005). Crime prevention through environmental design. *Security Technology and Design*, 36–42.
6. Crowe, T. D. (2000). *Crime prevention through environmental design*. Woburn, MA: Butterworth-Heinemann National Crime Prevention Institute, p. 36.

# Electronic Security System Integration

Physical security is the heart of healthcare security. There simply is no substitute for the professional expertise and human touch of security officers in the healthcare environment. But carefully selected and properly applied electronic security technology is playing an increasingly important role in safeguarding healthcare facilities.

The threat of terrorist attacks, an increase in weapons being brought into healthcare facilities, possible occurrences of infant abductions, and data security requirements of the Health Insurance Portability and Accountability Act (HIPAA) are keeping all eyes on the effectiveness of security programs in the healthcare environment. Thus, it is not surprising that most healthcare organizations turn to technology to supplement their existing security programs to make their security staff more productive and effective while reducing operating costs and limiting liabilities.

The IAHS has developed a basic industry guideline on the integration of electronic security systems in the healthcare environment.

## IAHSS HEALTHCARE BASIC SECURITY GUIDELINE, #08.01

### **Electronic Security Systems**

STATEMENT: Healthcare facilities (HCFs) will develop an electronic security system plan to provide guidance and direction for existing and future electronic system enhancements.

#### **INTENT:**

- a. Electronic security system implementations and enhancements are implemented after conducting a security risk assessment, often after an adverse event.
- b. An electronic security system plan should provide guidance for those involved in designing or enhancing the HCF's protection systems (e.g., security professionals, design and planning staff, architects, healthcare facilities administrators).
- c. Properly designed electronic security systems should augment and improve the effectiveness of staff resources.
- d. Electronic security systems should deter and detect criminal activity and other undesirable activities.
- e. Electronic systems can be a useful after-the-fact investigative tool.
- f. Whenever reasonably possible, electronic security systems should be planned and implemented in an integrated manner. For example, local door contacts or other alarms



should be integrated with closed-circuit television (CCTV) cameras. Alarm activation should automatically be integrated with CCTV monitors and allow persons monitoring cameras with a view of the alarm location.

- g. Electronic systems should be tested on a regular basis.
- h. Electronic systems should be installed and maintained in compliance with applicable life safety and building codes.

**Approved:** January 25, 2006

There are many technologies that can aid healthcare security staff in preventing crime and managing incidents. The key electronic security systems most frequently integrated into the healthcare protection program are intrusion detection, access control, and video surveillance. Today's security technological advancements in each of these areas and other applications enable higher degrees of security in the healthcare environment without compromising aesthetics, customer service, user friendliness, or overall hospitality. Unfortunately, too many healthcare organizations do not proactively approve electronic security capital expenditures until something occurs. In the 2007 IAHS survey of healthcare organizations, 22% of respondents who reported a spike in spending for electronic security technology in the previous year answered that they did so because of incidents or threats.<sup>1</sup>

A term endemic to any discussion of electronic security safeguards is systems integration. Many subsystems are purchased and maintained as stand-alone technologies, creating many challenges and difficulties when the system is needed to work with one another. A move toward designing these multiple subsystems to work together as a master or integrated system continues. Systems integration, thus, entails that either the subsystems operate from a single platform or the subsystems work together to achieve efficient monitoring and cost-effectiveness. The healthcare security administrator should make sure that the system is flexible and that it will meet current and future needs.

And while integration can be carried beyond the security level to include environmental controls, fire, and energy management, it is not recommended except in very small facilities. There are, however, opportunities for dual, or redundant, monitoring between separate security and building management/engineering systems.

Integrating security technology in the healthcare environment requires the blending of good facilities management, information technology (IT), and the latest security best practices. All three of these aspects of hospital management have an important part to the overall security and asset protection of the organization. Facility management plays the role of maintaining access control and CCTV hardware (as well as others) and IT has a role to implement and upgrade security software. It is the central role of the healthcare security administrator to blend the two for a cohesive protection package.

## Security Master Plan

One of the biggest obstacles facing healthcare organizations, as it pertains to their use of today's security technology, is the lack of understanding by the end user as to the capabilities of the system purchased. Frequently absent is a security master plan documenting the underlying electronic security philosophies that have been put into place by the facility. The security master plan should provide operating principles that help select needed security system capabilities and in turn guide appropriate security staff training and policy development. Championed by the security administrator, operating principles should not be created in a vacuum. Their creation should include key constituents of the organization to include representatives from the emergency department, IT, human resources, facilities, and risk management.

Take for instance the building perimeter system; it includes life safety and emergency communications, with consideration of employee and public entrances. When addressing the perimeter of the building, a common methodology is to break down healthcare entries into three categories:

1. *Employee entry*: For better separation between staff and visitors, entries should be electronically access-controlled. Access control software can also be integrated in the payroll system for better employee accountability and an incentive to use the designated employee entry point.
2. *Life safety egress doors*: Life safety code mandates the need for quick and uninhibited egress for employees, patients, and visitors. These doors need access control system contacts that signal door ajar, open door, and other situations.
3. *Patient doors*: Patients and visitors need to enter where they are greeted and directed to their destination. The University of Colorado Hospital in Denver is perhaps a role model in using signage, greetings, customer service, and access control as an effective means of achieving a secured facility.

Once each door is defined, the appropriate technology can be applied to ensure that it operates in accordance with the need. Patient/public access portals are typically open but need controls in place to secure in the event of an emergency. An open and inviting entry point atmosphere is desired as well as a goal to help visitors and patients get to their destination quickly and without confusion.

However, employee entrances typically require a different approach. Securing these doors at all times and equipping them with bypass technology provide employees with necessary access but deny entry of unauthorized personnel.

The primary purpose of life safety-focused doors is to provide emergency egress, not access. Equipping them with short-cycled closures and supervising them with door contacts (alarms) that inform security personnel of a breach can save thousands of dollars by foregoing the installation of expensive card readers and electronic hardware.

Simple but effective methods help guide the purchase and installation of security technology. In many instances, they augment security staffing but can, in some instances, substitute for staffing.

The security master plan should address replacement issues due to product expiration and the advent of new technology. The plan should address the integration of different systems, their compatibility, and how to maximize their capabilities. Like the facility master plan, the security master plan should be forward looking and anticipate future changes to the HCF and the surrounding environment. The master plan should help prioritize security-specific needs and once approved, align electronic security enhancements with the organization's capital budget structure.

Healthcare organizations operating without a security master plan often find frustration in obtaining needed financial resources and a hodgepodge approach of security technology—each creates an undesired perception of security.

The security master plan, in its final format, affords additional protection as it helps document the why behind what is being done in the protection program. In the event of an adverse situation, the protection afforded by this alone is significant. It demonstrates the importance of personal safety and security to the organization and comprehensively documents all that has been accomplished in creating a secure organizational posture. It shows that security is taken with importance from the highest administrative levels.

## Security Design Considerations

New facility construction, expansion, and renovation are continuous and almost nonstop in the healthcare environment. The healthcare security administrator must be prepared to work with hospital engineers, project managers, and/or architects to incorporate the most operationally efficient and cost-effective security technology for the project and budget. This includes defining the specific operating principles and philosophies of space utilization that drive specific technology applications.

The philosophy of all security design considerations should be to help build an environment that is patient-focused and incorporates both physical and psychological deterrence methods. Understanding what services are being offered and the patient population being served in the planning and design stage is a critical component of security design. The type of patient will often drive the type of security. In suburbia, where much of the new hospital construction occurs, security may be behind the scenes and more focused on securing the perimeter than individual departments. Because of a different patient mix and neighborhood demographics, urban facilities may want to focus on creating an outward psychological deterrence and compartmentalize security sensitive areas within its own security perimeter.

Security design considerations should also consider the time frame the project will serve. Take, for example, an emergency department renovation projected to fulfill the organization's emergency care needs for the next 10 years. Two important considerations are the expected patient volumes (capacity) and the anticipated patient demographics

projected for the new department at the time of opening and at the end of its projected life. Awareness and anticipation of these important considerations are critical to the security design considerations provided. This includes how the department is compartmentalized, what departments it should be adjacent to (such as the radiology department), the location of triage, the potential use of metal screening, and other considerations, which are discussed in more detail in *Chapter 20, Security Sensitive Areas*. Planning for each consideration is an important component; for instance, metal screening is not desired initially but the changing patient demographics and volume may require future installation of this additional protection measure. Thus, the security administrator must consider where the magnetometer will be located; how visitors, patients, and staff will be queued; and where confiscated and temporarily held items will be stored; naming just a few issues that need to be incorporated in the initial design (but not installed). Many healthcare organizations have found that retrofitting the layout and design can be more than three times more expensive due to wire pulling, and the need to move doors and other fixed walls. As a result, the future posture of security may be compromised owing to the cost-prohibitive expense of the needed installation and retrofit. The forward-thinking security administrator will anticipate the future changes that may affect the overall security posture and include them in their discussions with administrative leaders and architects in the design stage of the new construction/renovation planning.

## The Central Security Station

The efficient operation of a protection system requires that there be a hub, or center of operations. In smaller facilities, this hub is likely to be the telephone operator, which is only marginally satisfactory but a necessity in the small organization. Generally, communications personnel resist the addition of security to their responsibilities. Without a central security station (post), the functions of lost and found, key control, alarm monitoring, visitor/vendor management, central records, and security officer deployment, to name a few, are difficult to manage.

### Advantages

One of the basic functions of the central security post is to handle security communications. To maintain a high level of protection, each employee must report problems and suspicious activity to security. The easier it is to contact security, the more the employees will be motivated to participate in the prompt reporting of incidents or requests for service. When a security officer or dispatcher answers the telephone, the communication is quite direct. Not only is quicker response time obtained for emergency calls, but also inquiries can be promptly handled without relaying messages. The monitoring and linkage with public safety organizations can also render their service more efficient.



FIGURE 18-1 Example of a hospital central security station (Courtesy of PELCO).

The functions assigned to the central security post vary from organization to organization, depending on the elements of the security program. In any case, the potential for a 24-hour post expands the alternatives for program planning. Figure 18-1 shows an example of a hospital central security station. The station monitors security, fire, and critical electrical/mechanical building functions, and also serves as the operational center for a variety of security and management services.

## Design

When a central security station involves many process control functions, such as alarms, video surveillance, radio, and general monitoring, the design of the station requires considerable planning. One area that is often neglected is the human factor, which must be integrated with the physical aspects of the equipment. There are considerable differences in the size of the personnel who will operate the center; thus, some averages must be determined. For example, a person who is 60 inches tall has a line of sight when standing of 56.5 inches; a 72-inch person has a line of sight of 69 inches.

In general, the distance averages noted in Table 18-1, which assume a seated shoulder height of 35 inches, can be used for planning sit-down consoles.

The horizontal and vertical sight recommendations are measured from a straight-ahead, level line of sight. Many dispatch console manufacturers provide for variable height consoles that are electronically controlled with memory to move up and down on the basis of individual dispatcher-desired dimensions. Temperature, humidity, ventilation, illumination, background noise, and sound absorption are also important factors to consider in the design planning process.

**Table 18-1** Planning Considerations for Sit-down Consoles

Sit-down Console Planning Considerations	
Keyboard/controls	25–26 inch reach
Benchboard height	25 inches minimum
Keyboard/counter depth	18 inches minimum
Benchboard to chair seat	7.5 inches minimum
Horizontal sight	45° maximum
Vertical sight	75° maximum

## Cost

The basic problem encountered in operating a central security post is the expense, particularly for the labor required to maintain the post 24 hours per day (this requires at least 4.2 FTEs). Even though significantly increased protection will result, the required funding can be difficult to obtain. In addition to labor costs, the implementation of a central station can involve an extensive capital budget allocation over several years. Prioritizing the services to be provided and realistically projecting the implementation of those services will help in justifying the cost and obtaining the necessary funding.

Proper planning can reduce the cost of a central station by reappraising the entire system and considering certain trade-offs. The first consideration is location. It is neither necessary nor feasible to find a basement room that can be fortified against an attack or severe storms just because it is available and is space no one else really wants. Instead, the post should be located in an area that requires the presence of a security officer and is accessible to employees and the public. Good locations include the entrance to the emergency room, the employee entrance, the loading dock, and even the front lobby. Central security posts situated in these locations perform a double duty. The officers assigned to the post can perform a traffic control and surveillance function while fulfilling the responsibilities normally assigned to the central security station.

If the station is located in an area that already has 24-hour security coverage, it might perhaps be established without additional personnel. Another approach is to look for an area that requires a part-time or full-time clerk performing a function in another facility department. It may be possible to integrate the clerk's role into the security function and divert more funding into the security budget.

### *Shared Central Station*

A number of larger healthcare systems have found a shared central security station a more cost-effective alternative than individual security centers at each system hospital. Whether using a wide-area radio network, a radio repeater system, or other forms of two-way radio communication, these organizations have found a cost-effective alternative

to managing this important function. Sharing the security dispatch function and alarm monitoring often provides for multiple dispatchers on duty at a given time, offering important backup in the event of an emergency as well as needed coverage during meal and rest periods. In Denver, Colorado, the HSS Inc. operations support center provides a centralized solution for security-related telephone calls, alarm monitoring, emergency communications, and radio dispatching for the majority of the metro Denver area hospitals. The centralization expedites information sharing, speeds up officer response times, and makes it easy for hospital staff and visitors to contact security. The service allows for the organization to specialize in the specific business of healthcare and train dispatchers to deal with security and emergency-related issues when employees, staff, and visitors request or require security service.

A few healthcare organizations share the central security station with other ancillary/support departments such as facilities, IT, and/or environmental services. This system is not recommended as it is often found that call operators lack understanding of the criticality of the calls for service received.

## Alarms

A basic component of most electronic security programs is an alarm system. Alarm systems have many fire detection and warning applications; however, the discussion in this chapter is limited to the application of alarms for security surveillance, response, and control purposes.

The use of security alarms in the healthcare environment continues to increase, as it should. Properly planned, installed, and used, the alarm system is a very cost-effective component of the proactive security system. Cost-effectiveness is greatly enhanced when alarm systems are designed and installed as part of new construction or renovation projects.

The factors that limit the use of alarms include limited availability of capital funds, lack of monitoring capabilities, lack of knowledge, absence of administrative or physician acceptance, imagined or real employee morale problems, and the lack of innovative thinking on the part of protection administrators.

The security costs and the need to justify the budget force security administrators to recognize that a proper balance between labor and physical security is mandatory. Proper balance is the key phrase as alarm applications are primarily designed to render security personnel more effective. It is, however, possible that alarms and other security hardware components can reduce the total number of security personnel required for a given complex by increasing the productiveness of the security system.

In planning alarm systems, the concept of security as a system of perimeters, as discussed in *Chapter 17, Physical Security Safeguards*, may be helpful. The first concern is the outermost section of the building. The perimeter protection includes fences, windows, doors, roofs, and the like. Working inward, the next concern is area protection, which may be a room or a series of rooms, such as a pharmacy, general storeroom, or

medical records area. The next concern is point protection. The point may be a safe, vault, office machine, or even a piece of art. One hospital had so many thefts of artwork that it installed magnetic alarm switches behind each picture.

## Alarm System Components

An alarm system is composed of three interrelated parts: the sensory device, the transmission medium, and an annunciator. The sensory device determines that a potential problem exists, generally through an electrical circuit that is either open or closed. The types of change that an alarm system can detect include vibration, sound, and motion; a break in an electrical circuit; a change in pressure; the interruption of an energy beam; and a capacitance change due to the penetration of an electronic field. Each type of alarm has various applications in the healthcare setting. Each sensory device is often referred to as a point, and an alarm system monitors or supervises a number of these points.

The transmission of the sensory device signal to the annunciation point is usually accomplished by hard wire, telephone lines, or radio waves. The transmission medium must be monitored for line trouble or attempts to circumvent the alarm system. The security of the transmission medium must not be overlooked in the proper application of an alarm system.

The third component of the alarm system is the annunciation, or reporting, point. The annunciator, sometimes called a monitor, is a visual or audio signaling device that indicates the condition of the alarm circuits. Annunciation is usually accomplished by the activation of a signal lamp, visual display, printout, audible sound, or any combination of these elements.

Annunciation may occur in several places. A local alarm announces the signal in the immediate proximity of the area or item being protected. This announcement may be by bell, horn, light, or other means. For example, a local alarm might have a bell placed next to the door, protected by an electromagnetic switch. This type of annunciator is used more as a deterrent to scare off intruders than as a system to apprehend intruders. Some systems activate a voice message that tells intruders that they have entered a secure area and warns them to turn back. Of course, any message can be generated in this audio-type system.

A central station installation transmits the signal off the property and may be coupled with a local alarm annunciator. The central station is a remote, off-premises monitoring point. This system, generally provided by a commercial service, is specifically applicable to the medical office buildings, retail pharmacies, and clinics, which, when closed, likely do not have the benefit of onsite security personnel. Central stations are seldom located in the community where the alarms originate. There has been a tremendous consolidation of central stations, resulting in very large operations in various cities. It is not uncommon for an alarm system to be monitored a thousand miles or more away from the point of origin.



Some central station systems are approved by Underwriters Laboratory (UL). The central station of an alarm company that offers a UL-approved system must be located and built to fairly rigid UL specifications. UL approval is not necessarily required for most healthcare alarm applications, and the services of a non-UL-approved alarm company may even be superior to those of a UL-approved central station.

## Basic Alarm Applications

The two basic security alarm applications found in healthcare facilities are the intrusion alarm and the holdup alarm, or panic alarm. The intrusion alarm is used for sensitive areas within an HCF that are closed for certain periods, including clinics, pharmacies, laundries, general stores, medical records, libraries, and gift shops. The intrusion alarm is also a primary safeguard utilized for satellite pharmacies, off-site facilities, and medical office buildings.

The holdup alarm is frequently used in cashier's offices, pharmacies, and gift shops. This type of alarm is more often used to summon security personnel to observe suspicious people or activities rather than solely as a holdup alarm. Thus, in the HCF, the term would more appropriately be referred to as a duress alarm. Duress alarms are used in behavioral health units, emergency departments, and remote work locations to summon both security officers and in some applications, medical assistance.

Most duress buttons (alarms) are hardwired and attached to a wall or desk at a fixed location. There is, however, a portable product that allows an individual to move about a given "protected area" so that the activation device can be carried or worn on the person. This wireless system generally operates using a radio frequency (RF). New technology applications have allowed for the duress button to be placed on individual workstations as an icon on the computer.

Simple intrusion detection is probably the most familiar concept of security technology for most people. Intrusion detection involves the use of door or window contacts, glass contacts, and motion sensor in combination with some type of audible alarm that sounds when a person has forced entry into a building or room. An alert is sent to the central security station to notify authorities of the time and location of the incident. Security officers typically respond in person to evaluate the situation.

This method of incident response can be adequate for detecting an event and quickly getting to the scene. The effectiveness of the response at the scene is dependent on the proximity of security personnel to the incident and the seriousness of the incident. Few would argue against the intrusion alarm as a necessary component of a security system, however, there is little in place that would deter people from committing a crime in the first place, with the possible exception that signage indicating an alarm system may have some preventive value.

Common agreement does not exist concerning the value of a panic button utilized as a holdup alarm. Some people believe that in holdups the perpetrator is likely to have a weapon and a response by the police or by security personnel will likely create a situation

that could result in injury or death. This theory advances the premise that if a holdup is in progress, the security system has failed to prevent the crime, and it has become a law enforcement situation.

The essence of this question revolves around the response to the alarm rather than the existence of the alarm. An alarm warning might signal security personnel to observe an area or to adopt positions that will be advantageous in a confrontation or for general surveillance. The safety of those in the area is the foremost concern, and it is far better to obtain a good description of the event than to risk injury or death.

A common issue with many duress alarms is for staff to be knowledgeable about the actual location of the alarm, when it is appropriate to use the device, and the expected security response. Healthcare workers in areas where panic alarms have been installed should be trained on the location of the alarm and actively participate in test signaling an alarm from time to time. When exercised properly, employee confidence in the security system grows. It also provides the security team the opportunity to help individual staff members establish a reasonable expectation of security or law enforcement response.

## Proprietary Alarm Systems

The proprietary annunciation system is similar to the central station system except that the monitoring function and sometimes the installation and service are provided by the organization that is being protected. In this system, the alarm terminates on the property, and organizational personnel handle response to the alarm. This response may be to notify the police or the fire department or to notify onsite security personnel. In many health-care facilities, this function is assigned to the telephone operator because the switchboard is a 24-hour service. In larger facilities and multiple-facility systems that operate a 24-hour central security post, this post is the terminal point for the alarm system.

## Duress Codes

Some healthcare security administrators support the use of duress codes. A duress code is simply a word or phrase that alerts the person being called that the caller is in some kind of danger. However, the high turnover of healthcare personnel suggests that such codes may do more harm than good. Their use depends largely on their application and the number of people involved. If a protection system includes a central security station that receives alarms and the personnel in the alarmed area are limited in number, duress codes might be a part of the system. On the other extreme, gift shops are often operated by volunteers; it is therefore generally difficult to inform everyone involved about a panic alarm and its use, let alone teach them about duress codes.

## False Alarms

False alarms should be analyzed to determine the validity of an alarm system. False alarms result more often from personnel errors than from malfunctioning equipment. Proper installation is a key element in preventing false alarms, and alarm activation devices

should be well planned to avoid the false alarm problem. Having too many false alarms tends to decrease the protection level. In some situations, alarm systems have been simply disconnected because the high number of false alarms rendered the system ineffective. Where the police are called, it is quite common for fines to be imposed when false alarms occur. A high number of false alarms will often alter the type of police response.

## Access Control

The healthcare environment and hospitals specifically, by their nature, are designed to be open and accessible to the sick and injured and to family and friends, which means criminals and other dangers can easily enter through their doors if not properly protected.

Healthcare facilities face escalating security challenges in the 21st century. Today's older designs are too open and allow too much accessibility to walk-in patients and visitors without any kind of record or accountability. Good security design and electronic access control technology can significantly reduce this area of concern.

Access control, arguably the most critical aspect of protecting a healing environment, must start with critical thought to the design. The goal is to allow patients/visitors to move freely without feeling oppressed while protecting both guests and staff. Access control can protect critical areas such as pharmacies, surgery rooms, infant treatment rooms, technology closets/rooms, information storage rooms, and areas that separate staff from the public. Not only does it protect staff, it safeguards assets as well. The general public enjoys a greater degree of protection knowing parking facilities are monitored and the flow of patient/visitor traffic is limited, observed, and monitored.

Protection is important to every healthcare administrator, but it is incumbent on the healthcare security administrator to properly manage the first view patients and visitors have of the facility. That means access control systems used should not display a predominance of unfriendly barriers or obstructions. A defined philosophy of "on stage" and "off stage" is an important consideration in the design. Defining and separating out areas that are open to the public and those that are not are important first steps. Once identified, determining the level of security access, its level of sophistication, and restrictions to apply to areas that are not open to the public follows as the next step.

The results of the continued acts of violence and terrorism in the aviation and education sectors have pushed heightened security in operations and design. The healthcare environment is believed by many protection professionals to be just one incident away from following the direction these two market sectors have taken to improve security and specifically access control. The lack of media attention to the violent acts that continue to occur in the healthcare environment will not continue perpetually. Take for instance the March 2008 shooting spree at Doctor's Hospital in Columbus, Georgia. A gunman allegedly distraught over his mother's dying at the hospital in 2004 brought three handguns to the fifth floor and shot a nurse and an administrative assistant, before he gunned

down a patient waiting outside in the parking lot. Outside of the local community and state media coverage, there was minimal attention brought to this horrific incident by the national and international media.

With the anticipation of increased media attention to the growing levels of violence in healthcare and the general openness of the environment will come administrative pressure to control access beyond what occurs today. The healthcare security administrator must give forethought in the design to how access will be controlled to the environment as a whole. The main entrance in particular is a concern, as most hospitals specifically have very limited control of who comes and goes through this entry point during normal business hours.

## Electronic Access Control Systems

Electronic access control measures do more than just open a door. They allow or deny access to individuals on the basis of the organization's needs. The software programs at the heart of these systems allow security administrators the ability to determine who gains access, at what time, and on which specific days/dates. Security or other staff utilize password-protected software for audible alarms of intrusion, and develop reports for access control activity in the facility. Activity may include identifying individuals that attempt to gain access to locations off limits, as well as identifying doors that are left ajar or need mechanical attention.

Today's electronic access control programs can protect "itself from itself" by requiring double or triple authentication for access. Lost identification cards are no longer feared when biometrics or personal identification codes can be required to accompany the card to gain access to those areas that require the highest levels of restricted access, such as the pharmacy, narcotic dispensaries, and IT server rooms.

These software systems can be monitored by security staff in a secure room, produce reports, or send an alarm to a patrol officer to respond at the time of the occurrence. Table 18-2 lists three of the most common access control applications in the healthcare environment.

**Table 18-2** Common Access Control Technologies in the Healthcare Environment

Common Access Control Technologies	
Magstripe	Low cost; commonly used; not as secure as technology cards; can be duplicated easily; subject to physical wear and tear
Proximity	Durable; convenient; widely used for access control; more difficult to compromise or duplicate than magstripe technology but easier to compromise than contactless smart cards; less wear-and-tear issues
Contactless smart cards	Multiapplication functionality (access control, cashless vending, time and attendance); enhanced security through encryption and mutual authentication; less wear-and-tear issues; not as widely adopted as magstripes or proximity cards <sup>2</sup>

## Security Sensitive Areas

Section EC 1.2 of TJC compliance manual requires that hospitals “have a plan to control ingress and egress from each defined Security Sensitive Area.” On the basis of the risk, this plan could include the use of electronic access control or screening personnel, appropriate signage, and/or staff monitoring. The protection of security sensitive areas will be discussed in greater detail in *Chapter 20, Security Sensitive Areas*.

## After-hours Access Control

After hours continues to be the primary time of risk in healthcare facilities. Having a single clearance point to areas such as the emergency department or other single designated point of entry is recommended to control access into the facility after normal business hours. Hospitals usually lock all entrances during the late-night hours and grant access into the facility through a defined approval process frequently managed by security staff. Using a screening system that channels authorized visitors to a specific entrance inside the facility, CCTV cameras equipped with an audio capability, and electric-strike door latches allows the security officer far removed from the entrance to authorize and grant access as required. Authorized persons can bypass the need for an operator to release the lock by use of a key electronic push-button, card access devices, or biometric technology.

## Restricted Access Capabilities (Lockdown)

One of the most fundamental concerns within an HCF is the ability to manage properly and swiftly serious emergencies. Frequently, this requires the ability to restrict access into the facility. Lockdown procedures dominate discussions relating to emergency preparedness for healthcare organizations. The ability to restrict access quickly has been at the heart of spending for electronic access control systems for the past decade.

How fast the HCF can be locked down is a key indicator for facility readiness to many internal and external disasters, riots, civil disturbances, and other workplace violence scenarios. Every medical institution is only as good as what has been rehearsed. It is imperative that hospitals and healthcare facilities practice their ability to restrict access to the facility using both “table-top” demonstrations as well as an annual drill—preparedness is paramount. In addition, the security department should test the time it takes to restrict access to high-risk departments and other buildings on and off campus. When exercising the organization’s ability to restrict access to the facility in an emergency, capability should be evaluated at all times of the day to include weekends and holidays. If all tests are conducted at three in the afternoon when staffing in the facility is at its peak, a true test has not been completed. Coordinating scenarios to test available resources when security officers are engaged with a patient in the emergency department or during a fire drill is strongly encouraged.

It is the avid recommendation of many security professionals that medical facilities work in tandem with local authorities to address these issues, test the program, and make necessary improvements where needed. For instance, the use of the word lockdown is tossed around vicariously, but this term means for the institution to take serious measures in the event of a crisis. A lockdown translates into doors locked, lights dimmed, no traffic in or out of the building, and all staff to stay in their present location at the time of the lockdown. Many locations may heighten their security and restrict access because of an event within or near the institution, but with regular activity continuing.

Restricting access to the entire hospital has become more common to protect patients and staff. A two-stage process can facilitate crowd control during a lockdown, as follows:

- *Stage 1:* Specific entry/exit points are locked and a physical presence (such as a security officer) may be required.
- *Stage 2:* All perimeter doors are locked or staffed.

Electronic access control systems are increasingly used for these functions, with wireless or hardwired duress and lockdown buttons provided for key personnel to close and lock Stage 1 and Stage 2 doors. Most electronic access control software permit the system administrator to lock all controlled doors for both entrance and egress from interior doors, and exterior doors can be locked from an outside entrance. With locking hardware and/or magnetic locks, a building could be secured from the control room within minutes.<sup>3</sup>

## Intercoms/Video Door Phones

Often used to enhance electronic access control systems and integrated with video surveillance, a properly designed intercom system allows a visitor to be properly identified, and with the push of a release button, the staff member can unlock the door and permit access. Most important, these systems add an important convenience factor to the access control system and are frequently used by physicians and other care providers who may forget their issued access badge.

Video door phones display an image of the visitor shown in real time on the phone's monitor and a built-in microphone and speaker on the unit to let the staff member communicate with visitors. Authorized visitors can then be granted entry with the push of a single button. The application is commonly used for exterior entrances, parking garages, human resource departments, hazardous waste containment areas, or security sensitive areas such as the pharmacy, emergency care, maternity units, or health information management departments. The system can help prevent accidental and/or unauthorized entry to susceptible and prohibited areas.

The use of these systems in parking garages has accentuated the ability to call for assistance in the event of serious trouble or if troubleshooting needs to occur with a gate arm. Instant communication at ticket stanchions, parking garage stairwells, and other

locations within a parking structure have proven useful in maintaining a positive perception of safety in many healthcare protection programs.

Intercom systems are frequently used in assisted living or long-term care facilities in which housing or other living arrangement for the elderly, infirm, or disabled is provided. Commonly installed inside the resident's quarters, the intercom/video system can provide the opportunity to clearly identify visitors before permitting entry into the building or apartment. The systems can also be equipped with emergency pull cords to provide instant communication capabilities as well to ensure that residents have vital and constant access to assistance at all times.

## Managed Access Control

The concept of managed access is an emerging service that dovetails into central station services. The outsource management of the access control function is an alternative for many stand-alone clinics or smaller healthcare organizations who do not have the capital resources to install a sophisticated access system or the staff resources to manage the system daily. The managed access program can relieve a lot of up-front burden on the organization and continuing cost of ownership. However, to the end user, the door controls work the same. Typically, these systems work best in organizations that are controlling between one and eight doors.<sup>4</sup>

## Video Surveillance

Video surveillance systems have evolved significantly in the last several years. Older video systems needed banks of videotape for continuous recording, and required manual administration to swap tapes periodically during the day. Record keeping was prone to errors and finding specific incidents on tape was time-consuming. Digital video recorders (DVRs) and CCTV cameras have made significant advances in features and functions, taking advantage of fast computer processes and high-density storage media to digitize, compress, and record video from analog cameras.

Video surveillance, access control, and alarms have much in common, and they often work together as an integrated system to keep intruders out of secure areas, limit access to infant and pediatric units, and remotely monitor critical areas to reduce the risk of crime and security incidents. It is why more and more healthcare organizations continue to increase their use of video surveillance as part of their overall security plan. Integrated together, the technologies help to render security personnel more effective, and they generally require monitoring and response. Some video surveillance systems, however, are intended to only capture (record) images to be utilized later if necessary. In these systems, there may or may not be any live monitoring involved.

DVRs and Network Video Recorders (NVRs) have many advantages over older analog recording technology. Streaming video can be continuously recorded and discarded in cycles of days, weeks, or months if no security incidents occur. If an incident does occur,

disk indexing and time-stamping make it simple to find video from a given date and time. In addition, because the video is digitized, it can be exported and distributed via e-mail or backed up on CD, DVD, or other digital media using common computer backup programs that are widely available. The IAHS has developed a basic guideline on the use of video surveillance in the healthcare environment.

#### IAHS HEALTHCARE BASIC SECURITY GUIDELINE, #08.02

##### **Use of CCTV**

**STATEMENT:** Healthcare facilities (HCFs) will develop a policy to provide guidance and direction pertaining to the consistent managing of the application, control, authorization, and use of video images. CCTV is generally utilized as an after-the-fact investigative tool and when properly installed may serve as an effective element of crime prevention.

##### **INTENT:**

- a. Each HCF should determine the requirements for security cameras in facilities on the basis of security risk assessments.
- b. Authorized site personnel will have the ability to observe video images of public areas via live viewing or have the ability to review recorded images for incident investigation.
- c. Each HCF shall have a standard governing the protection of confidential information and images obtained from the use of CCTV, so that personnel use the CCTV system only for its intended purpose.
- d. Requests for an archive record of video images made by a law enforcement agency or other external agency will be directed to the person responsible for the security function, and may be granted if the request conforms to appropriate privacy and HCF standards.
- e. The person responsible for the security function should develop adequate measures to protect the information or images obtained from security cameras and establish a process so that information or images are observed, recorded, or shared only with persons entitled to receive such information.
- f. The use of covert cameras may be authorized in certain circumstances and under strict controls by the person responsible for the security function (see Guideline 04.01 Covert Investigations).
- g. Signage can be posted at the entrance of the facility where visible security cameras are utilized, indicating the presence of video surveillance equipment.
- h. When integrated with security systems (e.g., alarm contacts/points, intercom, or other devices), CCTV effectiveness can be greatly improved.
- i. Privacy protection measures are necessary to ensure that the collection of personal information by means of CCTV is lawful, justifiable, and that such information obtained is appropriately processed.
- j. The HCF's policy on CCTV should identify a minimum of 10 days for a retention period for recorded images.

**Approved:** February 2009



## Basic Use of Video Surveillance in the Healthcare Environment

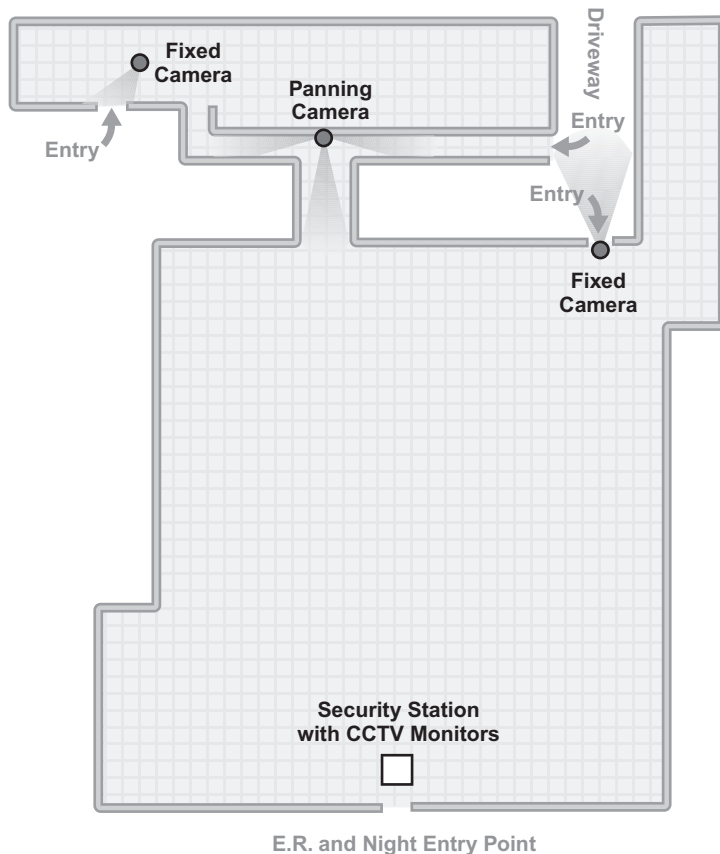
The challenge for healthcare security professionals is not to fully understand the electronics of video surveillance, but to be innovative in applying this physical safeguard to the management of vulnerabilities. Video surveillance has two basic security uses: access control and general surveillance. In healthcare security programs, video surveillance has primarily been used for surveillance; however, access control applications are increasing. These access control applications may be found at emergency room entrances, receiving dock gates, physician offices, computer rooms, pharmacies, and basic building or parking access points.

Live monitoring of video surveillance equipment is a greater problem than monitoring alarms, at least for general surveillance. A person generally cannot view a monitor for more than 30 minutes without becoming bored and ineffective. Security experts in all industries agree that it is physically impossible to look at more than one camera at a time. Even if multiple views are squeezed onto large monitors, they would be rendered unusable for detection of most criminal activity or other malfeasance.<sup>5</sup> However, there is no standard rule on how many cameras operators can view at any one given time. Many video surveillance systems are thus integrated into the protection system so that constant viewing is not required nor intended.

Event-driven monitoring of CCTV systems has come into greater use. This monitoring equipment alerts the operator when the monitor must be viewed. In these systems, the monitor to be viewed will often be automatically shifted to a larger screen and will activate the recording equipment. Occasionally in large security programs, this technology is integrated with the electronic access control system and called *video verification*. The integration of these two systems, for example, allows a user to see live video as well as the cardholder's picture when a given access card is presented at a reader. The security staff can verify that the person presenting the badge is the actual cardholder. Another example of video verification occurs in identifying individuals who are "tailgating": when one person swipes their badge and gains access to the facility and another person follows them in without presenting their badge. The integrated system allows organizations to visually identify, verify, and capture security breaches at access points.<sup>6</sup>

General surveillance is one of the basic uses of CCTV. When used for this purpose, the system is perhaps more of a psychological deterrence than an actual physical control. The configuration of the three cameras in Figure 18-2 was designed to protect the access points of the west side of the facility while a security officer at a monitoring station physically controlled access on the east side of the facility. The east side has the emergency room entrance and the night staff entrance.

CCTV is increasingly being used for security in decentralized systems. The responsibility for certain aspects of security is returned to the operating or functioning level of a department. An example would be a loading dock that requires surveillance during receiving hours to determine who is coming and going and to address the vulnerability of unattended shipments on the dock for short periods of time. The materials management



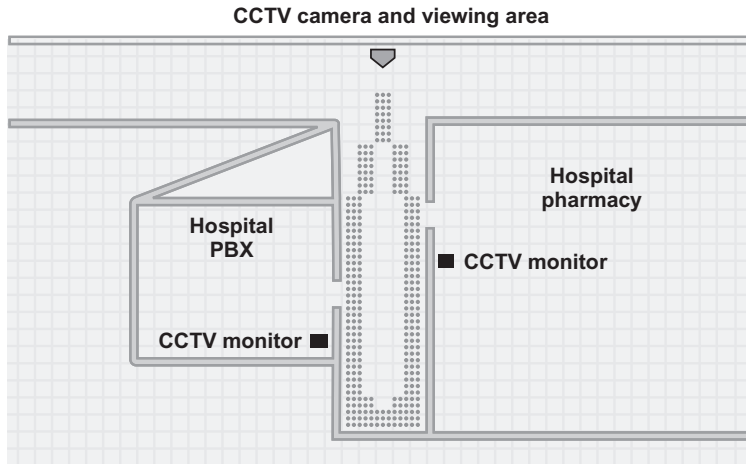
**FIGURE 18-2** Example of using CCTV to protect one side of the facility with a security officer controlling access and monitoring cameras on the opposite side.

department could monitor the dock with CCTV. A monitor could be placed on a secretary's desk or at another point within the department. This type of installation is quite economical as compared to transmitting the signal back to a central security station.

Another example of the decentralized approach is to place a camera in the corridor just outside the main pharmacy employee service door. The monitor is placed inside the door, permitting pharmacy employees to view the corridor before opening the door to exit.

In the decentralized design shown in Figure 18-3, one camera can be viewed by two different operating departments. Employees working in both the telephone switchboard room and the pharmacy can view the common corridor before exiting from their respective workstations.

In the United Kingdom, the National Health Service has deployed cameras in their emergency wards and in ambulances in an effort to cut the rising levels of violence against NHS staff. The cameras are designed to collect evidence and prosecute people attacking NHS staff.<sup>7</sup> Brian Main, the security manager at Ninewells Hospital in Dundee,



**FIGURE 18-3** An example of the use of CCTV for security purposes in a decentralized configuration.

Scotland, believes that the extensive CCTV coverage deployed at his hospital has resulted in the people responsible for committing offenses to be swiftly identified and brought to justice.<sup>8</sup>

In the United States, the Federal Bureau of Labor Statistics reports that healthcare professionals who deal with behavioral health patients, work in admissions, emergency rooms, and crisis and acute care units along with emergency medical response teams experience the largest number of assaults.<sup>9</sup> Properly located video surveillance cameras can extend the range of the security staff and provide valuable incident information.

To increase staff safety, recommended camera locations in the healthcare environment include

- Main entrance of emergency rooms, waiting rooms, and nontreatment areas within the examination/treatment space;
- All hospital entries; visible public monitors also offer a deterrent;
- Admissions desks and elevator banks;
- Where controlled substances are present, to include the pharmacy and narcotic dispensaries;
- Receiving docks and other locations storing items of value;
- Mother/baby, pediatric, behavioral health, and geriatric units, to help prevent abduction and patients from wandering off;
- Parking lots and garages have high pedestrian traffic and often have many hiding places for an attacker to hide.<sup>9</sup>

A study conducted by the University of Berkley of the Community Safety Cameras deployed in the city of San Francisco found no evidence of an impact that the strategically deployed cameras had on violent crime. However, the study found “statistically

significant and substantial declines in property crimes within view of the cameras,” pointing to a significant deterrent effect cameras have on property crimes.<sup>10</sup>

Spartanburg Regional Healthcare System, in Spartanburg, South Carolina, found out that the video surveillance does not deter all violent crime as footage was recorded of a man cornering a woman in an elevator and using an intimidating presence to rob the woman. However, the video from the hospital released to the police and to local media outlets resulted in arrest of the suspect.<sup>11</sup>

## Equipment

The most important consideration in a video surveillance system is the quality of the image received, and this is largely dependent on the camera. The major factors crucial to picture quality are amplitude response, signal-to-noise ratio, resolution, horizontal aperture correction, sensitivity, and transfer smear. Comparing these qualities in relation to the price will provide the right camera for a specific application.

The transmission of the signal to the monitor also affects image quality. Although coaxial cable is widely used for analog cameras, CAT 5 cabling is used for most IP cameras. A recent trend is that the cameras themselves have video processors, which can reduce network bandwidth requirement by sending high-speed, high-resolution images over the network only when required.

The size of the monitor should be based on the purpose of monitoring and individual preference. A general rule is to increase the size of the monitor as operator-viewing distance increases.

The charge-coupled device (CCD) is a widely used chip camera. Chip cameras generally do not need heaters, consume much power, or need a large protective housing. Despite some drawbacks in resolution and sensitivity, they have effectively replaced tube cameras.

Another major advance is the use of microprocessors and microcomputers in video systems. This technology allows systems that were formerly operated manually to be pre-programmed and automated. DVRs (with analog cameras) and NVRs (with IP-based cameras) are often used for forensic analysis of events. These products offer advanced video processing modules that can be applied in a hospital setting, including face and object recognition and crowd anomalies (e.g., someone leaving an object such as a backpack, people traveling the wrong direction, and motion detection).

In healthcare facilities where dependable surveillance is essential but price is often an object, the necessity of upgrading an existing CCTV analog system to match the digital equipment of the new system is often debated. Typically, when a new surveillance system is installed, the old system becomes a relic. During the transitional stage, typically, the healthcare organization must duplicate equipment rooms and terminal feeds. Providence Everett Medical Center in Everett, WA, when faced with the conversion of analog cameras to digital during a large renovation project, found that converting the analog signal to digital before routing to the DVR was a good first step. The organization created

an internal policy to replace all existing analog equipment as it failed, thus maximizing the functionality out of remaining equipment.<sup>12</sup> The different requirements for analog and digital surveillance equipment are significant. A comparison of the different system requirements is denoted in Figure 18-4.

### *IP Cameras*

Increasingly, electronic security systems are converting from analog to digital, Internet protocol (IP)-based equipment to provide and transport information that facility staff need to manage security threats. IP-based cameras are now more widely accepted and quickly becoming the standard in the healthcare industry. With digital, IP-based CCTV systems, camera images are now available anywhere the data network is available, unlike analog systems that generally require coaxial cable at each viewing location.

Besides providing a digital platform, IP cameras offer some real advantages over traditional analog cameras. According to Ben Scaglione, CPP, director of security at New York Presbyterian, Weill Cornell Medical Center, IP cameras:

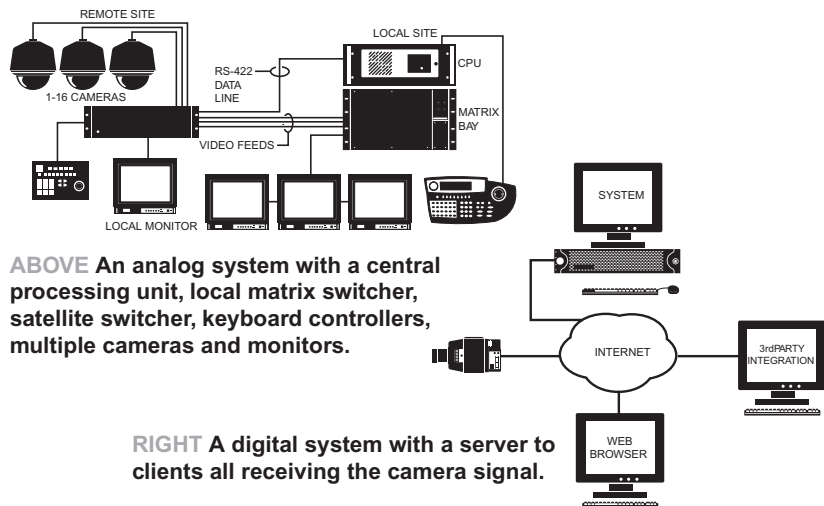
- Can be wireless;
- Can be powered over the network utilizing one cable for both power and video signal;
- Scalable, flexible, and allow for open architecture;
- Video is easily transferable to hard drives; searching and retrieving video is faster and easier;
- Come with high definition or megapixel capacity;
- Offer analytics that can be programmed into the camera, freeing up network bandwidth and improving storage and processing capabilities.<sup>13</sup>

For organizations that are installing 40 cameras or more, the cost for IP cameras is generally lower than analog cameras as labor costs offset the higher equipment costs.<sup>14</sup> There are five basic questions that every healthcare protection administrator should ask before embarking on an IP-based camera project:

1. *What are the IT department's network standards?* Every IT department has its own set of requirements for networks, cabling, hardware, and software. Be inclusive and get IT involved often and early.
2. *How are the cameras and software going to work together?* With the volume of IP camera choices, it is wrong to just specify only resolution and style. The chosen camera should have a proven track record for communicating with a particular software package. It is much easier to manage and support if all cameras on the network are by a single manufacturer.
3. *How critical is the recorded video?* Defining up-front the purpose behind collecting the video image as evidentiary, regulatory, or liability purposes will determine hardware and system configuration.

## COMPARISON OF ANALOG AND DIGITAL SURVEILLANCE SYSTEM REQUIREMENTS

Analog system requirements	Digital system requirements
Matrix switcher to control camera input/output; Signal splitter to determine number of camera views per screen; Amplifier to provide signal boost over long cable distances; Monitor (cathode ray tubes are being replaced by liquid crystal displays); and Keyboard/joystick controller to provide human-machine interface.	Server (on-site or off, dedicated or shared); and PC work station (all functions handled by PC).
Recording device (video cassette recorders are being replaced by digital video recorders).	Recording device (digital video recorder).
Six-conductor, 22-American wire gauge (awg) control wire; Two-conductor, 18-awg power wire; and RG59 U-type coaxial cable for signal.	CATS cable (all functionality and power is delivered through one cable).
Camera lens; Enclosure; and Pan/tilt mount.	Camera (commonly housed in a dome with pan/tilt/zoom on board).
Power supply (cameras typically run on 12/24-volt direct current power).	Network switcher (interface with local area network, collecting points and power to camera).



© COPYRIGHT of Pelco, Inc., All Rights Reserved, 2009. Reprinted or portions reprinted with the permission of Pelco, Inc.

**FIGURE 18-4** Comparison of analog and digital surveillance system requirements (Courtesy of PELCO).

4. *How long does the video need to be available?* Most storage calculators have four variables including: frame rate, compression type, hours of camera operation, and the average percentage of activity or motion the camera will experience on a daily basis. In any case, the calculation is not an exact science but the requirements should not exceed 75% of the storage device upon installation.
5. *Does the system need to be scalable in terms of adding cameras to the system in the future?* The server configuration must have enough horsepower so that the processor does not exceed 60% of its capability. The type of camera chosen and the compression technology selected are the two drivers of this load factor.<sup>15</sup>

Analog cameras continue to have an advantage over IP cameras, especially in specialty applications. Infrared (IR) cameras, for example, use IR lighting so even where there is no, or low, ambient light, the IR image is still available. Wide dynamic cameras balance backlight with images in the foreground so both are visible. These products are good for lobbies where there is bright light outside but the inside is relatively dark. The specialty analog cameras can be incorporated into IP video systems through the use of encoders. Encoders can also be used to connect older analog cameras to IP systems when cost is a concern to replace legacy camera systems. Systems that use both IP and analog technology are commonly called hybrids.<sup>16</sup>

### *Video Analytics*

From its inception, video analytics has been touted as a solution to assist those providing security to critical infrastructures with a powerful means for identifying and detecting intruders, tracking people or objects, and producing an alarm on types of behavior. The benefits of video analytics have only started to be realized in the healthcare environment. For example, foot traffic in the evening past a closed pharmacy may be considered normal. But, lurking near the pharmacy door may be an indication that a break-in is about to happen. Another example of applied video analytics is a fence-climbing alarm. Security staff may know that it is common for people to walk along the outside of a fence, horizontally across the field of view. They are typically not concerned, as it poses no threat. Yet, if someone were to begin to climb the fence, producing vertical motion across the field of view, this is deemed as an alarm, and video is transferred to the security central station.

Expectations about the productivity improvement to be derived from using video analytics must be addressed up-front. There are video analytic products that can do amazing things but some do no more than basic motion detection. If video analytics are used, the healthcare organization must know and plan up-front how to use a system. Knowing the threat or risk to be managed is critical in setting up these systems.

Many healthcare organizations that have installed this new technology have had preconceived notions of how video analytics can bring reductions in security staffing or increase the effectiveness of deployed security officers. Rarely do these assumptions

prove true. In many instances, the video analytic product can actually increase the burden on the security department. The Universal Security Systems' guideline is to expect one false alarm per camera per hour.<sup>17</sup>

Many of these systems claim to work right out of the box. However, there are more variables and perimeters in video analytics than other camera solutions. Proper design is the only way to help avoid these errors and their increased cost of ownership, which includes:

- *Lighting issues:* Not enough light causes poor camera quality; light in the wrong places can produce shadows, glare, and dark spots.
- *Detection ranges:* Know how many pixels on target the system requires and design the camera coverage accordingly.
- *High false alarm rates:* Wind in many regions can cause false alarms as can sun glare, shadows, and the presence of other nuisances.
- *Transmission issues:* Weak networks, wireless links, and improperly terminated video cable can create headaches.<sup>18</sup>

### *Thermal Imaging Cameras*

Thermal imaging cameras provide the ability to look at any structure and see the slightest shift in temperature and spot leaks, ruptures, hot spots, animals, and intruders. This technology allows security personnel to detect threats without the need for natural or artificial illumination and works in all types of weather and lighting conditions. The application is not widely used in the healthcare environment, but has application in laboratories, IT server rooms, and other high-value asset protection where subtle differences in appearance cannot be detected through traditional camera systems.

### *Covert Cameras*

Covert cameras can be a very useful tool in the investigative process but must be used with discretion and appropriate administrative approval. According to Dave Mongeau, CPP, a healthcare investigator with 30 plus years experience, one of the more common covert cameras is the “smoke detector” camera. This camera has been available for years and has proven to be very useful as most employees rarely notice their existence. This particular style of covert camera provides the end user an unobstructed view of a very large area when used with a wide-angle camera lens. Another useful covert tool is “Micro DVRs,” about the size of a deck of cards, when used with double-sided tape. These devices can be installed in seconds. Most frequently used in the motion-detector mode, these devices can be very useful during after-hours in an office experiencing theft problems with minimal after-hours activity. The micro DVR is not, however, a good tool for areas with high activity.

A large number of covert camera styles are available off-the-shelf, such as the “pencil-sharpener” and “clock” cameras. Custom-built covert camera enclosures have been created for many specific applications and limited only to the creativity of the requesting party and the resources available to mitigate the risk.



Evidence collected during the covert investigation should be reviewed with the human resources department if the situation involves an employee. If a criminal act has occurred, chain of custody regarding the captured images is an important consideration should the healthcare organization pursue prosecution. The security administrator should be responsible for the chain of custody and the required written documentation.

## Recording

As a general rule, all cameras utilized in a security system for after-the-fact investigation and overall deterrence should be recorded and the recording retained in a 10-day library as a minimum. It is not uncommon to maintain recorded images for 30 days. There are, however, two known exceptions to this basic healthcare security industry guideline.

The first exception is the use of video surveillance in patient care areas or for patient monitoring. Of great debate among many healthcare providers is whether the recorded video image is a medical record. Various interpretations of the HIPPA regulations yield differing opinions. One interpretation is that the recording should be a part of the medical record and stored accordingly with health information management. Other healthcare professionals feel that the only documentation needed in the medical record is that the image has been recorded. To date, there is no clear direction on which interpretation is correct. The security administrator involved with determining the stance of an individual healthcare organization is encouraged to engage the privacy officer, risk management, and legal counsel. Regardless of which direction is chosen, the organizations should clearly choose between these two distinct interpretations, clearly document its policy and procedure, and consistently follow the practice as written.

The second exception is the use of video surveillance solely for the control of access into a secured unit/department. Take, for example, the pharmacy; cameras may be deployed and integrated in an intercom system used to talk with and identify a staff member requesting entry into the department. In this application, the camera's sole purpose is to identify who is being granted access into the department and not for collecting a recorded image. Some healthcare organizations have chosen to record cameras used for this basic purpose. However, it is not an industry standard practice.

In short, the driving purpose for the use and application of the video surveillance should govern whether or not it is recorded. The purpose and use should be documented in the security master plan.

## Monitoring

A major question regarding the use of any CCTV is how the cameras will be monitored. The answer, of course, depends on the application. There are many combinations of monitoring, from a dedicated security person centrally monitoring the system on a full-time basis to no live monitoring at all. In the case of no live monitoring, the cameras are simply recorded for future viewing if necessary. There are partial viewing and redundant (two or more viewing locations) monitoring models as well. Redundant monitoring is

generally reserved for specific strategic cameras and is most often found in video surveillance systems that utilize both a centralized and decentralized design model. An example of redundant viewing would be the facility birthing area. It is common to install a completely self-contained system for this area being monitored on the unit. Only certain cameras would also send signals back to a centralized security monitoring point.

In programs that do not have full-time security officer monitoring, it is common to locate the video monitors at the facility telephone switchboard. In this application, the monitors should be set on a shelf that is tilted down and faces the operators. They should not be so high that the operators must constantly strain to look upward. This positioning saves space and allows the operators to make normal eye contact with the monitors while they carry out their primary duties. In some programs, security alarms and the security radio system are also controlled from the main switchboard. A problem arises when the operators are reluctant to take on this additional responsibility. Telephone operators, who are on duty 24 hours a day, are often given many extra responsibilities and therefore can be overloaded.

Another area for monitoring is the engineering control room found in many modern physical plants. Electrical, mechanical, water conditions, and other functions are monitored in this room. This location may also provide an acceptable place for monitoring security equipment and/or be a backup area for security monitoring should the primary security monitoring equipment malfunction or in the event the control center would need to be evacuated.

## Video Surveillance in Patient Care Areas

The use of video surveillance cameras is no longer just a security function and limited to the protection of the facility; it is also used to support patient care efforts. Healthcare organizations are deploying cameras to help with telemedicine, quality management of surgeries, patient safety, and remote monitoring of patient behavior.

The Children's Hospital of Wisconsin created a virtual Intensive Care Unit capability using 72 pan-tilt-zoom cameras that enable their physicians and other healthcare staff located elsewhere in the hospital complex to observe and zoom in to see what is happening in each patient room. The cameras, equipped with intercom capabilities, provide for two-way visual and audio interaction. The cameras in these patient rooms do not record to ensure privacy and the video data travels over separate network to maintain complete patient confidentiality.<sup>19</sup>

Lancaster General Hospital in Pennsylvania has added CCTV cameras to all 42 operating rooms. Placed in the center of the main surgical light, the camera provides everyone in the room with the surgeon's view, including nurses, anesthesiologists, and other medical personnel. A patient safety-focused initiative, the fewer people going in and out of the surgery room has lowered the risk of infection. Physicians also use the video to discuss a particular case with other physicians as well as use the video images to teach academic courses.<sup>20</sup>

According to Dr. Tracy Buchman, Director of Safety and Emergency Management at the University of Wisconsin Hospitals and Clinics in Madison, video monitoring of activities in patient rooms and patient areas is permitted in five situations:

1. *Undisclosed clinical monitoring.* Conducted as a purely clinical endeavor for patient safety and to assist in diagnosis. An example is clinical suspicion of Munchausen by Proxy Syndrome.
2. *Undisclosed law enforcement monitoring/recording.* Conducted with an appropriate court order authorizing the activity.
3. *Department of corrections.* Monitoring of the locked department of corrections unit and patients in its custody.
4. *Disclosed video monitoring with consent.* Conducted with written consent of patient or the patient's representative. For example, when it is needed to monitor the behavior of staff or visitors other than the patient's representative.
5. *Hospital legal department approval.* Situations not noted that may have a legal basis for monitoring. Special authority does not exist to authorize monitoring. The purpose is to determine if there is some legal basis for providing approval.

Many organizations also monitor patient behavior in the emergency department or in the behavior health units remotely. CMS is specific in their expectations of healthcare organizations and expect staff to take extra care to protect the safety of the patient when interventions that are more restrictive are used. Specifically, CMS requires continuous monitoring and if conducted remotely, must include both audio and video monitoring equipment. The staff member monitoring the patient using the audio and video equipment must be in close proximity to the patient and their monitoring must be uninterrupted.<sup>21</sup> Cameras installed in observation rooms in either the emergency department or in the behavioral health unit should be vandal-resistant. There should be no way for a patient to grab hold of the camera because of how it was made or installed.

Some healthcare organizations have used infrared cameras to monitor patients in their sleep lab. The camera can operate in the dark and its use in sleep studies has proven invaluable as care providers can monitor patient sleep patterns without disrupting the patient.

Healthcare organizations that authorize video monitoring of patients typically require the video to be watched at all times. Many organizations require, by policy, that monitoring and recording be stopped at all times if it is not monitored. There should always be a means for the person watching the video to promptly notify clinical personnel if a potential intervention is required. The recording of the video monitoring should be kept in a secure location, used only for the purpose for which it was recorded and not be released, used, or disclosed to others unless approved by the organization's administrative or legal department.

### Dummy (Fake) Cameras

No discussion of CCTV would be complete without some mention of the so-called dummy camera. There is no question that some of the value of CCTV for security applications

is the psychological deterrent it creates. Malefactors are never quite sure how many cameras are there and who is watching their movements. It therefore stands to reason that a fake television camera would provide a possible deterrent of a negative act.

Unfortunately, it is extremely difficult to avoid revealing that the dummy camera is not real. Opponents argue that because the dummy camera cannot be kept secret, it implies to employees that the organization is “playing games” with them. If security controls are to be administered on a positive rather than a negative basis, there is little use for fake cameras.

The strongest argument against the use of the dummy camera is that it can create the expectation that one is being protected when in fact no protection is being provided. This may produce a situation in which a person takes chances or invites trouble on the basis of their false sense of security. A false sense of security can also exist when real CCTV systems are not monitored or do not function as intended. The concept of false security has been the basis of many lawsuits, for example, *Cisky v. Longs Peak Association, et al.* (84 CV 5668) District Court, Denver, Colorado, wherein the plaintiff was awarded more than \$6 million by a jury. The issue in this case was, in part, the question of a camera that did not provide the protection that was indicated.

## Other Security Technology Applications in Healthcare

There are numerous other technologies used in the healthcare environment to protect people, safeguard assets, and protect the reputation of the organizations. These include visitor management systems, infant protection systems, emergency call boxes, mass notification, asset tracking, and metal screening.

### Visitor Management

Visitor management systems are not new to the healthcare industry as patient rosters and paper guest logs have been used at information desks to help with way-finding and guidance for years. What is new is the computerized way to capture detailed visitor information and to accurately identify, badge, and track visitors, vendors, and other authorized personnel entering the HCF and the purpose of their visit.

With a standard personal computer and inexpensive label printer, these systems allow users to fill in a simple visitor form on the screen, and then print a high-quality, customized badge for each visitor. Today, most visitor management systems are integrated with a number of peripheral hardware devices, such as passport scanners, driver's license readers, business card scanners, digital cameras, electronic signature capture pads, proximity card readers, fingerprint readers, and barcode scanners.<sup>22</sup> The use of a camera also allows the healthcare organization to capture the visitor's photo. And when vendors are required to read and agree to a Non-Disclosure Agreement or Confidentiality Statement, or any other document, the more sophisticated visitor management systems can capture the visitor's signature electronically as part of the visitor record. That signature can be linked to the type of document that was presented, read, and agreed upon.

One of the greatest benefits of the more advanced visitor management systems is the ability to incorporate programmable security alerts or watch lists. An important alert checks each visitor's name against a list of people who should not be allowed to enter the building (former employees, estranged spouses, etc.) and alerts the security officer or greeter when a match is found, telling them how to handle the situation.<sup>23</sup> The visitor management system in use at The Children's Hospital in Denver checks each name against the state's sex offender lists and alerts security if a match is found. A positive match does not necessarily prevent entry, it will however require a security escort while in the hospital.

Another advantage found with most of these systems is the "Emergency Evacuation" report that provides a list of who is currently in the facility that needs to be accounted for in the event an evacuation is required. Some systems even allow this list to be automatically e-mailed to external fire, police, and emergency response personnel.

### *TJC Surveyor Identification*

With The Joint Commission (TJC) now conducting all regular surveys, imposters have turned up in a number of hospitals claiming to be Joint Commission surveyors. The reasons for attempted entry into the healthcare organization are many and range from the unscrupulous to the criminal—gaining faster access to care or faster access to a family member, to stealing prescription drugs. As news reports of these events have shown, such events can have dire consequences for patients and compromise public trust.<sup>24</sup>

Joint Commission surveyors follow established procedures when visiting an organization to conduct an unannounced accreditation survey and are trained to expect hospital personnel to make inquiries to verify their identity. Surveyors will report to either the front desk or to hospital security upon their arrival and will voluntarily present identification. To confirm authenticity of the badge that surveyors wear when they visit a facility for survey, organizations may compare it to a sample posted on The Joint Commission extranet site.<sup>25</sup> Table 18-3 demonstrates actions to be taken to verify surveyor identity.

**Table 18-3** TJC Survey or Identity Verification

#### **TJC Surveyor Identity Verification Checklist**

- Request to see The Joint Commission Surveyor badge
- Compare the badge present to the sample badge on the TJC extranet
- Verify survey date on the extranet
- Verify assigned surveyors on the extranet
- Ensure that employees know what actions they should take if they have concerns about someone entering the organization
- Direct questions about the veracity of a surveyor to Joint Commission account representative at 630-792-3007

*Courtesy of Joseph Cappiello, vice president for Accreditation Field Operations at The Joint Commission.*

## Infant Protection Systems

Infant abduction prevention is a top concern for hospital administrators, and security of infants is certainly a priority, both for safety and public relations reasons. All told, 126 newborns have been abducted from hospitals since 1983.<sup>26</sup> “Infant Tagging,” as it is often called, is a high-tech infant protection program designed to prevent baby abductions from infant care units, nurseries, and found more and more frequently in pediatric units. Typically, a small round button-like tag attached to a band is placed around an infant’s ankle or wrist soon after birth. Each tag is actually a miniature RF device that works in conjunction with the access control system and automatic door locks. An alarm sounds when a tag approaches or goes through a door. An active monitoring system reports where a tag is at all times by sending a signal to the central monitoring center at the hospital.

Electronic infant protection systems range from basic systems that sound an alarm when an infant is taken into certain areas to computer-based systems that identify and track infants, lock doors and elevators, and provide timed alarm activation. A basic design of each system is to allow the baby’s parents or authorized hospital personnel to carry the baby freely throughout a designated area without generating an alarm. However, if an infant is brought near an exit door it locks, or if the band is tampered with, an alarm is activated.

Hospitals are increasingly integrating electronic infant security systems with access control and CCTV systems. If the system is integrated with the access control system, all doors leaving the area automatically lock (in coordination with fire safety) and control elevators. An integrated system can also link infant handling to access cardholders, activate CCTV cameras, and lock stairwell doors. Some infant tagging systems have features that can also immediately display the identification of the baby and a map locating the exit door through which the baby was taken and track the tag throughout the facility.

Challenges of installing these systems may include differentiating portal and tamper alarms, properly testing the system, and managing nuisance alarms. The volume of “false alarms” continues to be the greatest staff concern when using these systems.

Infant tagging is useful in preventing newborn abductions, but it is not foolproof. Cathy Nahirny, Administrative Manager with the National Center for Missing and Exploited Children, has documented 14 cases where an infant was abducted by a non-family member from an HCF and the facility had installed an infant security tagging system.<sup>27</sup> Eleven of these occurrences have occurred since the last writing of this book.

Infant protection systems, video surveillance, and controlling access to prevent unauthorized visitors from gaining access to the mother/baby unit must work collectively together and in conjunction with staff training, parental education, and a critical incident response plan. We will explore infant abduction prevention and response in greater detail in *Chapter 20, Security Sensitive Areas*.

## Emergency Call Boxes

Emergency phones, call boxes, phone towers, or wall-mounted emergency phones are all names used to describe the emergency phone system designed to connect a potential

victim of crime or someone in need of service with security. No matter what they are called, most emergency call boxes share the same or similar features, including the user interface and electronics that go into them. Some models contain an automatic dial-up telephone where phone service is provided at each unit. Others contain an intercom-style speakerphone equipped with one, two, or more buttons.<sup>28</sup> Most emergency call telephones are equipped with a blue-light strobe on top of the device to enhance visibility. When flashing, it helps expedite security officer response and let others in the vicinity know that assistance is needed.

Direct communication with the central security station or PBX operator is the most common application for transmitting the call signal and provides direct two-way communication with the call initiator via a direct phone line, voice over internet protocol (VoIP), cellular application, or two-way radio. Most systems available generate a campus map at the remote monitoring point providing specific location information of the call box, even if the call initiator cannot wait on the response. Thus, a security officer can be immediately dispatched to the location of the originating unit.

There are several variations of emergency call boxes to choose from, including a fairly wide variety of colors. Most fit into two basic groups—wall mount and tower—and are readily identified with the words EMERGENCY or HELP. Wall mounts are generally deployed where ceiling height is limited, such as inside a parking garage. Towers are free-standing devices that are often strategically located in surface parking lots and other high pedestrian-traffic areas on campus. Both serve a common purpose: provide immediate assistance to those requesting it. Figure 18-5 is a picture of a typical tower-style emergency phone used on many healthcare campuses.

Emergency phone systems are also used for nonemergency purposes and can be excellent customer service tools for employees, staff, and visitors who may need basic assistance. These devices, when used, are excellent crime prevention and public relations tools as they demonstrate organizational commitment to a safe and secure environment. They also provide an added visual reinforcement of being protected.

## Mass Notification

Healthcare facilities have traditionally relied upon overhead announcement for alerting staff of threats and other items of public concern. There are codes for tornados, fires, bomb threats, and security assistance. In the past, it was not uncommon for a hospital to announce “paging Dr. Strong” whenever security was needed to handle a violent situation or other calls for security assistance.

The 2007 Virginia Tech University tragedy served as a wake-up call for many healthcare facilities and has yielded numerous lessons learned that has prompted hospitals, behavioral health treatment centers, and long-term care facilities across the country to reassess how they prepare for, respond to, and mitigate incidents of targeted violence. Specifically, this tragedy identified the need for the HCF to have a quick and facility-/campus-wide notification of a threat or emergency.



FIGURE 18-5 Sample emergency phone tower.

Technology advances have provided many mass notification solutions available to the HCF. In many instances, the use of e-mails and pagers has supplanted overhead announcements; however, many healthcare organizations have realized that multiple modes of notification are needed to reach all the constituents inside the facility and on its grounds. Figure 18-6 provides a listing of the many different types of mass notification systems available to the HCF, with the advantages, disadvantages, and applications.

## Asset Tracking

Losing wheelchairs or diagnostic equipment to theft is a great expense and significant risk for healthcare organizations. Recently, many hospitals have started to protect their assets with wireless radio frequency identification technology (RFID), which uses small transmitters attached to the protected equipment that communicate with the organization's access control system. Similar to the unobtrusive security tags used on store merchandise to thwart shoplifters, RFID tags are often used to track equipment as it moves through various doors and can detect where a piece of equipment is located within the organization or if it leaves the facility. RFID tags range in size from small chips to palm-size plastic boxes. In short, an RFID tag can be attached to just about anything of value, such as an EKG monitor or mobile workstation, and can be easily tracked throughout the facility.

Some hospitals are wary of using RFID because of concerns about potential interference with critical equipment. A study published in the June 2008 issue of the *Journal of the American Medical Association* reported that RFID tags could interfere with the functioning of medical devices.<sup>29</sup> The observed problem was more common with passive



SOLUTION	STRENGTHS	WEAKNESSES	APPLICATION COMMENTS
<b>Bullhorns</b>	<p>Inexpensive</p> <p>Can operate when there is no power</p> <p>Easy to use</p>	<p>Limited to small areas of coverage</p> <p>Challenges with voice intelligibility</p> <p>Require much personnel to operate</p> <p>Potential for misuse by unauthorized personnel</p>	<p>Be certain batteries are always charged</p> <p>Good for evacuations for foreseeable events (hurricanes, tornados, etc.)</p>
<b>Call Boxes</b>	<p>Since they are already installed on many campuses, the technology can be repurposed to push information out</p> <p>Individuals located in the area of a call box can communicate with law enforcement, and police/security can pinpoint their location</p> <p>No sign-up required to receive messages</p> <p>Constituents are familiar with this type of technology</p> <p>Strobes that are normally installed can alert hearing-impaired</p>	<p>Challenges with voice intelligibility</p> <p>Volume of speakers may not be loud enough for individuals standing away from the devices to hear an announcement</p> <p>Normally not designed for communications inside buildings</p> <p>Cost due to hardwiring or maintenance</p> <p>Designed for 9-1-1 calls and assistance calls, not to be a warning device</p> <p>Depending on the model, messages may not be able to be catered to specific areas</p>	<p>Normally deployed in parking lots/garages, public thoroughfares, remote areas and other outside locations around campus</p> <p>CCTV/security cameras can be installed on them for additional situational awareness</p> <p>Speakers can be installed for mass notification</p> <p>Wireless units can overcome some cost/installation issues</p>
<b>Digital Displays (changeable message signs, LED signs, LCD signs, etc.)</b>	<p>Portability</p> <p>No sign-up required to receive messages</p> <p>Reach hearing-impaired</p> <p>Good return on investment if used regularly for non-emergencies</p> <p>Integration with other emergency alert solutions</p>	<p>Can be costly on large campuses with many rooms or due to hardwiring or maintenance issues</p> <p>Can be overlooked if not used regularly or placed properly</p> <p>Portable units can take time to deploy</p> <p>Many are not CAP compliant</p>	<p>Good for traffic control, crowd control and alerts during major events (football games, etc.)</p> <p>Can be deployed inside buildings (classrooms, hallways) and public areas (cafeterias, student unions)</p> <p>Used for everyday routine kinds of communications. People look at them and expect to get useful information</p>
<b>E-mails</b>	<p>Can leverage pre-existing e-mail system</p> <p>Effective for messages going to staff who have computers controlled by the facility</p> <p>Constituents can't opt out of the system</p> <p>Communicates with off-campus constituents</p> <p>Can be used for non-emergency communications</p> <p>Integration with other emergency alert solutions</p>	<p>Reliability. Not everyone checks their e-mails immediately (message recipients may be in class, with a patient, or away from their desks or PDAs for some reason)</p> <p>Server overloads may result, causing delays in message receipt</p> <p>Messages may be mistakenly classified as spam by recipients or third-party servers</p> <p>Often follow-up messages can't be sent until the initial e-mail is delivered</p>	<p>E-mails can be prioritized so they get through faster</p> <p>Divide recipient list into appropriate groups (e.g. by campus) and when possible, only send messages to affected individuals</p> <p>Know how many e-mails per minute your network can handle. Too many could overload the system</p> <p>Test the system regularly</p> <p>Educate message recipients on how to sign up, what they should expect and how to configure their spam filters</p>
<b>Intercoms</b>	<p>Good return on investment</p> <p>Familiarity in the healthcare environment</p>	<p>Many are not CAP compliant</p> <p>Not supervised, so facility personnel do not always know when system in disrepair</p>	<p>Used frequently in hospitals by employees, a higher level of training can be achieved, making the system very effective for mass communication during emergencies</p>
<b>Loudspeakers (fixed or portable, aka "Giant Voice")</b>	<p>Inexpensive</p> <p>Cover a large area</p>	<p>Dead spots</p> <p>Challenges with voice intelligibility</p>	<p>Increase effectiveness by combining with strobe lights to alert hearing-impaired</p> <p>If conducting a test and another area is in</p>

**FIGURE 18-6** Mass notification systems: advantages and disadvantages (Courtesy of Robin Hattersley Gray and Campus Safety Magazine).

SOLUTION	STRENGTHS	WEAKNESSES	APPLICATION COMMENTS
	<p>No sign-up required to receive messages</p> <p>Highly intrusive</p>	<p>Aesthetics (speakers are very large)</p> <p>Portable solutions can be expensive</p> <p>Unintended message recipients (e.g. Neighbors in residential areas)</p>	<p>earshot but is not the intended recipient, announce the test well in advance to prevent panic and unnecessary alarm</p> <p>Consider the topography of the area where the speakers will be deployed to get the maximum output so messages reach their intended targets</p>
<b>Phone trees/ telephony</b>	<p>Location and recipient specific</p> <p>Call receipt acknowledgement</p> <p>Compatible with major mapping systems</p> <p>TTY/TDD calling for the hearing-impaired</p> <p>Remote launching capability</p> <p>Can be used for non-emergency communications (attendance notification, outreach and important reminders)</p>	<p>Cost</p> <p>Database management</p> <p>Not appropriate for large scale notifications due to limited trunk or cell tower capacity - landlines and cellular providers might experience service failure/saturation during a major incident like 9/11 or Katrina</p> <p>Recipients may not be where the phone is located or phone may not be turned on</p> <p>Customer support for upgrades</p>	<p>Particularly effective for small scale mass notification (e.g. emergency team members, small communities, hospital staff) and during the evening/overnight hours</p>
<b>Popup message (banners) on computer screens</b>	<p>Allow messages to be displayed on computer desktops and PowerPoint presentations even if the user has not logged onto e-mail</p> <p>Intrusive</p> <p>Relatively inexpensive</p> <p>Messages can be discreetly specified for individuals or groups of persons</p>	<p>Currently not effective on computers that are not controlled by the facility, unless process established whereby message recipients can enroll to receive alerts on their computers</p> <p>Messages do not reach those campus constituents who are not logged onto their computers</p>	<p>Effective for messages going to employees and staff who have computers controlled by the campus</p>
<b>Posters</b>	<p>Placed in common areas</p> <p>Inexpensive</p> <p>Easy to create and deploy</p>	<p>Can be overlooked</p> <p>Can be slow to create and deploy</p> <p>Require much personnel to deploy</p>	<p>Create templates before incident occurs to increase deployment speed</p>
<b>Radio announcements</b>	<p>Can connect with campus and local police departments</p> <p>Inexpensive</p>	<p>AM coverage can be a challenge inside buildings</p> <p>Messages usually cannot be catered to a specific area; must be general</p>	<p>Create text for announcements beforehand. Be certain public information/communications department reviews verbiage</p>
<b>Sirens</b>	<p>Inexpensive</p> <p>Cover a large area</p> <p>No sign-up required to receive messages</p> <p>Highly intrusive</p> <p>Versions with strobe lights alert hearing-impaired</p>	<p>Dead spots</p> <p>Inability to communicate specific messages</p> <p>Limited indoor use</p> <p>Frequent tests required</p>	<p>Good for alerts</p> <p>A network of sirens can be deployed to overcome some dead spot issues</p> <p>Can be mixed with voice instruction and strobes for improved communication of specific information</p>
<b>Text (SMS) messaging</b>	<p>Effective way of communicating with off-campus constituents</p> <p>Text delivered via a separate control channel that is reserved for data only on cell networks.</p> <p>Solution uses much less bandwidth than voice</p> <p>Can be used for non-emergency communications (attendance</p>	<p>Messages may be considered spam by some systems and/or recipients</p> <p>Cost</p> <p>Registration required</p> <p>Database management challenges</p> <p>Limited by trunk capacity, which may slow delivery of message</p>	<p>Develop credibility of system and institution by only using it when appropriate; avoid overuse</p> <p>Test the system regularly</p> <p>Educate message recipients on how to sign up and what they should expect from the solution</p> <p>Database of intended recipients can be</p>

FIGURE 18-6 (Continued)

SOLUTION	STRENGTHS	WEAKNESSES	APPLICATION COMMENTS
	notification, outreach and important reminders)	<p>Messages cannot be catered to a specific area; must be general</p> <p>Some smaller, regional carriers don't have agreements with major carriers, which prevents the messages from being delivered</p>	<p>broken down by distribution groups to increase delivery speed</p> <p>Inform those who sign up to verify they have an SMS messaging plan, otherwise messages might not be delivered</p> <p>If using a third-party vendor, make sure they have made the appropriate arrangements with aggregators and cell carriers so their emergency messages won't be delayed or blocked</p> <p>Have the message originate from a campus rather than a vendor. This increases the likelihood that the message will be prioritized correctly</p>
<b>TV announcements</b>	<p>Inexpensive</p> <p>No sign-up required to receive messages</p>	<p>Messages cannot be catered to a specific area; must be general</p>	<p>Messages can be scrolled across screens; can interrupt regular programming if campus has control of cable system</p>
<b>Voice evacuation (connected to the fire system)</b>	<p>Technology can be repurposed for mass notification, increasing the system's return on investment</p> <p>Highly regulated by industry codes</p> <p>Fully supervised so facilities personnel are informed immediately when system or portions of system are not functioning</p>	<p>Mainly deployed indoors</p> <p>Voice intelligibility issues</p> <p>Does not reach hearing-impaired</p> <p>Potential NFPA code changes</p>	<p>External speakers off of a fire alarm voice evacuation system on the exterior of a building so people just leaving or approaching the building can be made aware that something is going on inside</p> <p>Combine with strobes to reach hearing-impaired</p>
<b>Weather radios</b>	<p>Preprogrammed to activate during weather warnings</p> <p>Can also send civil emergency messages</p>	<p>Announcements are usually not site- or campus-specific</p>	<p>Counties might eventually become subdivided so a campus can receive its own designation for alerts</p>
<b>Web announcements</b>	<p>Information can be updated quickly</p> <p>Leverage pre-existing campus Web site at no additional cost</p> <p>Good for communicating information to those outside of campus (visitors, media, etc.)</p> <p>RSS feeds can automatically populate social networking portals (Facebook, MySpace, Twitter, etc.)</p>	<p>Sites can become overloaded when there is a lot of traffic due to limited server capacity</p> <p>Web sites may not be regularly checked by campus constituents</p> <p>Is a passive information delivery mechanism; is not intrusive</p>	<p>Explore catastrophic bandwidth options</p> <p>Temporarily water down site (limit use of graphics and scripting) during emergencies so more people can access site without it crashing</p> <p>In hazard-prone areas, Web sites should be redundant, being hosted (as back-up) in an off-site area where there are no (or fewer) hazards</p> <p>Other mass notification systems often direct campus community to check Web site for additional information</p>
<b>800 numbers (hotlines)</b>	<p>Inexpensive</p> <p>Message center usually located away from area where disaster is occurring so the line remains functional</p> <p>Not limited by number of landlines on campus</p>	<p>Is a passive information delivery mechanism; is not intrusive</p> <p>Can be limited by local cell tower and other capacity issues</p> <p>Messages cannot be catered to a specific area; must be general</p>	<p>Particularly appropriate for providing information to those outside of affected area (parents, media, etc.)</p>

FIGURE 18-6 (Continued)

RFID tags, which are powered by the electromagnetic field of handheld tag-reading devices, than with active tags with their own power source, which operate at much higher frequencies, and have an expanded operating range.<sup>29</sup>

Video analytics have been used as an alternative to RFID for asset tracking. The camera can be programmed to highlight a piece of equipment, sense if the equipment moves, record when it does and alert security.

## Metal Screening

Philosophically, there are some healthcare environments that lend themselves to metal screening. The most likely application in a healthcare setting is in the Emergency Department.

Statistics illustrate that the emergency department encounters more violence than any other department or area of the facility, largely because of the variety of illnesses and injuries it treats and the diversity of the population it serves. Emergency departments by their very nature serve gang members, psychiatric patients, domestic violence victims, and others who may become irrational or dangerous out of fear, anxiety, or other factors. Moreover, because the order in which patients are seen often depends upon the severity of illness, waiting time can add to the tension and create security incidents.

The growing pervasiveness of violence has caused many hospitals to take significant measures to decrease and deter risks of violent activity in the emergency department. It is estimated by the American Hospital Association (AHA) that approximately 5% of people entering an emergency department bring in something that could be used as a dangerous weapon. In response, more and more emergency departments are using metal detectors.

The recommendation, introduction, and management of metal screening programs in healthcare cannot be done in a vacuum. The security improvements are considerable; however, the introduction of metal screening has employee relations and organizational culture implications in addition to patient and community perceptions that must be addressed collectively. The placement and exact location of the metal detector is an important consideration. The device should be installed to minimize unnecessary delays in the queuing of patients and visitors and to fit comfortably into the aesthetic décor of the facility.

Of particular importance to medical facilities is the electromagnetic interference (EMI) caused by the metal detectors. Pacemakers, defibrillators, nerve stimulators, and other medical devices may be inactivated or reprogrammed by this phenomenon. Instances of this happening have been extremely rare; however, studies conducted by the German Heart Institute in Munich, Germany indicate that EMI is not as likely to occur as common wisdom would lead us to believe.<sup>30</sup>

If metal screening is employed, the approach must be consistent and show no bias. The traffic flow should be streamlined so that persons cannot bypass or divert the process, unless the patient is unstable. All unstable and ambulance-transported patients deemed “at-risk” should be scanned using a hand-held wand once it is medically safe to do so.

A drawback to implementing a fully operating metal detection system is the staffing requirements. The passage of patients and visitors through the metal detector must be managed without interruption to include relief for meal and work breaks.

## Testing of Security System Components

Many electronic security systems are used to keep healthcare facilities safe. But one of the common missing components is the routine testing of these systems. Systems or components are commonly found to be ineffective, not working as originally intended, and/or not meeting current needs—creating unnecessary risk and liability exposure for the healthcare organization.

A strategy that works particularly well is to assign someone on staff who, at least on a monthly basis, takes an inventory of all equipment in use, verifying its operational status. If equipment is found missing or not operating as originally intended, document those issues and place them on the internal work order plan to correct the deficiency. This close-the-loop system must be followed to ensure that systems are working and ready when needed.

This documentation and testing may be considered small and routine. However, its importance is found in the liability protection afforded to the facility and more prominently, the positive perception of security and the department.

## Security Technology Implementation Tips

Implementation of new or upgraded security technologies requires the same basic preparation. The following guidelines will help the healthcare protection professionals ensure a more secure environment:

- Engage the healthcare organization's IT staff early and often to ensure that the cabling, networking, and software support resources are available and reliable as the plan is implemented and used in real-life situations.
- When evaluating intrusion detection, card access control, and video surveillance systems, it requires vendors to demonstrate how integration of these security functions can increase security and minimize the training and burden to security personnel.
- Avoid “bells and whistles” and cutting-edge products that have not been proven; focus on smart purchases and user-friendly applications.
- Ensure that adequate space, reliable electrical power, and sufficient cooling are provided for each component of the electronic security support system.
- Clearly delineate in the organization's security master plan whether the security or IT department has authority for equipment and ongoing maintenance.
- Maintain thorough records of electronic security system components, including component labeling, location, cabling types, cable termination information,

equipment cut sheets, node and port IDs, application software routines, and IP addressing and network configuration information.

- Engage in ongoing training on new systems and upgrades.

The ideal healthcare security system is a combination of the right technology, careful planning, proper installation, and a strategically deployed staff. Technology must work effectively as a tool for a well-trained security staff. When these elements are properly integrated, the organization is able to provide a safe environment, and its employees are consequently able to concentrate on fulfilling the organization's overall mission of providing high-quality patient care for the surrounding community.

## References

1. Blesch, G. (2008, June 30). First, do no harm. *Modern Healthcare Special Report*, 28.
2. Hattersley-Gray, R. (2007, September/October). Exploring your access control options. *Campus Safety Magazine*. Retrieved January 12 2009, from <http://www.campusafetymagazine.com/Print/?ArticleID=126>.
3. Canal, B. A., & York, T. W. (2009). Decreasing the risk of emergency. *Facilities Management Journal*, 22–28.
4. Hodgson, K. (2009). The new kid on the block: Managed access. *SDM*, 55–58.
5. Donald, Dr. C. (2009, May). Optimizing camera viewing in control rooms. *Hi-Tech Security Solutions*. Retrieved May 30, 2009 from <http://www.securitysa.com/article.aspx?pkIArticleId=5627&pkICategoryId=3>.
6. Van der Merwe, N. (2009, May). Integrated health care. *Hi-Tech Security Solutions*. Retrieved May 30, 2009 from <http://www.securitysa.com/regular.aspx?pkIRegularId=4011>.
7. Tindle, G. (2009, April 24). CCTV cameras to curb violence against NHS staff. *Wales Online News*. Retrieved April 25, 2009 from <http://www.walesonline.co.uk/news/wales-news/2009/04/24/cctv-cameras-to-curb-violence-against-nhs-staff--91466-23463081>.
8. CCTV Reduces Crime in Hospital. (2008, September 13). *BBC News*. Retrieved September 13, 2009 from [http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk\\_news/scotland/tayside\\_and\\_central/7558455.stm](http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/scotland/tayside_and_central/7558455.stm).
9. Brisbee, F. (2000, April). The power to heal and more. *Electrical Contractor*. Retrieved May 23, 2009 from <http://www.ecmag.com/index.cfm?fa=article&articleID=10050>.
10. King, J., Mulligan, D., & Raphael, S. (2008, December 17). *CITRIS Report: The San Francisco Community Safety Camera Program*, 11–12. Retrieved January 13, 2009 from <http://www.citris-uc.org/files/CITRIS%20SF%20CSC%20Study%20Final%20Dec%202008.pdf>.
11. Peters, C. (2009, March 7). Man caught on tape just before garage robbery. *Spartanburg Herald Journal*, Spartanburg, SC. Retrieved March 8, 2009 from <http://www.goupstate.com/article/20090307/articles/903071031>.
12. Tunnell, G. R., Jr. (2008). Moving to digital. *Health Facilities Management*, 21(9), 33–37.
13. Scaglione, B. (2007). Digital security technology simplified. *Journal for Healthcare Protection Management*, 23(20), 56.
14. Engebretson, J. (2009). State of the market: Video surveillance. *SDM*, 57–58.

15. Kuhn, M. (2009). 5 Questions for a successful deployment of an IP video solution. *SDM*, 78–80.
16. Hattersley-Gray, R. (2008). Making the leap to IP video: A safer bet. *Campus Safety*, 22–23.
17. Steele, J. (2009). Learning to deploy analytics. *SDM*, 61–64.
18. Steele, J. (2009). Learning to deploy analytics. *SDM*, 66.
19. Children's Hospital of Wisconsin deploys DVTel solution. (2009, January 7). *IP Security Watch*. Retrieved January 8, 2009 from <http://www.ipsecuritywatch.com/article/printer.jsp?id=14897>.
20. Wolf, S. (2008, June 27). High-tech health. *Central Penn Business Journal*. Retrieved June 27, 2008 from [http://www.centralpennbusiness.com/print\\_article.asp?aID=66929](http://www.centralpennbusiness.com/print_article.asp?aID=66929).
21. Centers for Medicare and Medicaid Services. (2004). Interpretive guidelines. §482.13(f)(4)(i)(ii). *State Operations Manual*, 112–113.
22. Landro, L. (2008, November 17). The hospital is watching you. *The Wall Street Journal*. Retrieved November 17, 2008 from <http://online.wsj.com/article/SB122645364411819495.html>.
23. Marson, H. (2007, September/October). Say goodbye to your paper guest log. *Campus Safety Magazine*. Retrieved June 6, 2009 from <http://www.campussafetymagazine.com/Articles/?ArticleID=121>.
24. Cappiello, J. (2007). Imposter surveyors: The joint commission urges hospital caution. *Journal for Healthcare Protection Management*, 23(2), 19–20.
25. Cappiello, J. (2007). Imposter surveyors: The joint commission urges hospital caution. *Journal for Healthcare Protection Management*, 23(2), 21–22.
26. Raburn, J., Jr., & Nahirny, C. (2009, March 24). Newborn/Infant Abductions. *National Center for Missing and Exploited Children*.
27. Nahirny, C., & Ryce, J. (2009, March 27). Infants Abducted from Hospitals with Security Tagging Systems. *National Center for Missing and Exploited Children*.
28. Colombo, A. (2006 May/June). Call box basics and beyond. *Campus Safety Magazine*. Retrieved June 6, 2009 from <http://www.campussafetymagazine.com/Articles/?ArticleID=34>.
29. Stiles, S. (2008, June 25). Interference with ICU-type medical devices seen from radio-frequency security tags. <http://www.TheHeart.org>. Retrieved June 25, 2008 from <http://www.theheart.org/article/print.do?primaryKey=877949>.
30. Jimenez, A. (November/December 2006). Metal detection worth its mettle. *Campus Safety Magazine*. Retrieved April 22, 2009 from <http://www.campussafetymagazine.com/Articles/?ArticleID=64>.

# Preventing and Managing Healthcare Conflict and Violence

Ever since it became a hot topic in the 1990s, the term *workplace violence* has referred to violence involving one or more employees. Despite the thousands of pages written on workplace violence, there is no concise definition for it. For most security professionals, it means any act of physical violence, threats of physical violence, harassment, intimidation, or other threatening, disruptive behavior that occurs at the work site. Workplace violence can affect or involve employees, visitors, contractors, and other employees.<sup>1</sup>

Richard Hampton, Head of Security Management for the National Health Service (NHS) Security Management Service (SMS) noted that one of the first charges of the SMS when introducing a national strategy for healthcare security in the United Kingdom was to define *physical violence*. Before the formation of the SMS in 2003, the NHS was using approximately 20 different definitions with no standard definition of abuse and no robust process for collecting data on violence against NHS care providers.

Workplace violence is an industry-wide healthcare problem and not exclusive to any one healthcare organization. Violence threatens the safety of staff, patients, and visitors in hospitals and healthcare organizations of all sizes and settings. It demoralizes healthcare professionals, especially nurses, who are most often the victims of violence, and costs hospitals untold millions in lost time, employee turnover, reputation for quality care, and additional security measures.

Regardless of the patient care services offered, the threat of violence in the workplace is all around us. A disgruntled visitor who is asked to wait several hours in the emergency department waiting room is only a moment away from violence, an at-risk patient who has an altered mental status could create a concern for violence, and the victim of domestic violence often has no choice but to go to the emergency department to receive care for injuries sustained. The scenarios are endless and real in the healthcare industry—no healing environment is immune from having violent acts occur inside the facility or on its campus. [Table 19-1](#) lists the wide examples of violence that can be witnessed in the healthcare environment.

The issue of violence is well known by the healthcare community, which has been seeking ways to combat it for years. But the violence continues to occur and is most prevalent in emergency departments, behavioral health facilities, waiting rooms, and geriatric units. Approximately half of the nurses responding to a 2007 survey conducted by the Emergency Nurses Association believe that violence is simply part of their everyday work environment.<sup>2</sup> In the survey, 9 out of 10 Emergency Department Managers cited patient



**Table 19-1** Listing of Workplace Violence Examples

Workplace Violence Includes	
<ul style="list-style-type: none"> <li>• Assaults</li> <li>• Stabbings</li> <li>• Suicides</li> <li>• Shootings</li> <li>• Rape</li> <li>• Attempted suicides</li> </ul>	<ul style="list-style-type: none"> <li>• Threats or obscene phone calls</li> <li>• Intimidation</li> <li>• Harassment of any nature</li> <li>• Being followed, sworn at, or shouted at</li> <li>• Psychological traumas</li> </ul>

violence as the greatest threat to department personnel. In addition, emergency department nurses reported<sup>2</sup>:

- Dissatisfaction with the overall level of safety from workplace violence (89%)
- Feeling unprepared to handle violence in the emergency department given their education and training (83%)
- Reduced job satisfaction due to violence (74%)
- Impaired job performance for up to a week after a violent incident (48%)
- Taking time off because of violence (25%)

Over 75% of surveyed emergency department physicians in Michigan said they had experienced at least one violent act within the previous 12 months.<sup>3</sup> According to the US Bureau of Labor Statistics, nurses and other personal care workers suffer 25 injuries annually resulting in days off from work for every 10,000 full-time workers—12 times the rate of the overall private sector industry. Fifty percent of nurses surveyed by the Massachusetts Nurses Association (MNA) and the University of Massachusetts said they had been punched at least once in a 2-year period. Twenty-five percent said they were regularly punched, scratched, spit on, or had their hand/wrist twisted. Some reported being strangled, sexually assaulted, or stuck with contaminated needles.<sup>4</sup>

Today, the term *workplace violence* continues to be expanded to include any act of violence in the workplace regardless of the connection of the victim or perpetrator to a specific business or employer. The California Department of Industrial Relations, Division of Occupational Safety and Health (DOSH), divides events of workplace violence into four categories: Type I, Type II, Type III, and Type IV:

- Type I event (*criminal*)—the perpetrator has no legitimate relationship to the healthcare facility (HCF).
- Type II event (*patient*)—committed by someone who is the recipient of a service provided by the HCF or the victim.
- Type III event (*employee*)—committed by someone who has an employment-related involvement at the HCF, such as current or former staff members.
- Type IV event (*domestic*)—relates to interpersonal violence at the HCF and includes spouses, lovers, relatives, and friends or other visitors who have a dispute involving an employee, patient, physician, or contractor.

One of the first in-depth reviews of violence in the healthcare industry was published in 1984 by James T. Turner. His book, *Violence in the Medical Care Setting: A Survival Guide*, has served as a basic resource for healthcare security administrators.<sup>5</sup> In addition to Turner's book, another authoritative book on the subject is Sandra L. Heskett's *Workplace Violence: Before, During, and After*. Although it is not exclusive to healthcare settings, Heskett does open her book by describing a violent hospital incident that occurred on June 20, 1994, at Fairchild Air Force Hospital in Spokane, WA. In the incident, a man recently discharged from the military used a Chinese-made MAK-90 to kill 5 people and injured 23 others.<sup>6</sup>

The majority of people generally associate violence in the workplace with assault and homicide, not with intimidating postures or expressions of mild anger. It is important that the healthcare administrator break workplace violence down into *actual* violence and the *threat* of violence. Both can create a hostile and uncomfortable work environment, and even with this breakdown, healthcare workers face significantly higher risk of injury from nonfatal assaults (actual violence) than that of other workers. The threat of violence, although not adequately tracked by most healthcare organizations, is also quite high in terms of threats of violence.

Violence is a major problem in all healthcare settings in all countries. More assaults occur in the healthcare and social services industries than in any other, according to a 1998 report published by the US Occupational Safety and Health Administration (OSHA). More than one in 10 NHS workers in the United Kingdom (12%) reported experiencing physical violence from patients or their relatives in a 2008 survey conducted by the Healthcare Commission—up 2% from 2007.<sup>7</sup> A report from Statistics Canada found that 34% of nurses in Canada had been physically assaulted by a patient in 2005. Those working in geriatrics and long-term care facilities were most likely to experience physical abuse, while registered psychiatric nurses were also particularly at risk. The statistics are similar to numbers released in the 2005 National Canadian Survey of the Work and Health of Nurses. That survey of nearly 19,000 nurses found that more than a quarter reported they had been physically abused by a patient in the previous year.<sup>8</sup> A 2006 Queensland (Australia) Nurses Union survey found that 45% of nurses had experienced some form of violence in their workplace.<sup>9</sup>

As concerning as the above statistics are for the healthcare industry, underreporting of violence is a chronic problem as a persistent perception within the healthcare industry is that assaults are part of the job. Underreporting is a concern by the SMS of the NHS where analysts studying the issue of physical violence against their healthcare workers steadfastly believe that violence is underreported by at least half. Many US hospitals have various reporting sources (Security, Risk Management, and Employee Health Departments) and multiple avenues for reporting events but often lack coordination between the reporting sources. Security is typically most focused on the event while Employee Health is focused on the employee. If the two databases are not coordinated, a large gap in the data can occur. The MNA is on record saying that violence is substantially underreported, in part because nurses are afraid it will show up on their performance

evaluation as not being able to appropriately handle a patient.<sup>10</sup> Other care providers purportedly underreport incidents of violence out of fear of reprisal, isolation, and embarrassment.

Why violence is so prevalent in healthcare is a question asked by many security professionals and administrators. According to the OSHA, healthcare and social service workers face a high degree of work-related assaults owing to the following risk factors<sup>11</sup>:

- Rising use of hospitals by police and criminal justice agencies for criminal holds and the care of acutely disturbed persons
- The early release from hospitals of acute and chronic mental health patients who have not received follow-up care and who can no longer be involuntarily hospitalized except in extreme situations
- The availability of drugs and money at hospitals, clinics, and pharmacies, which makes them targets for robbery
- Situational factors such as open facilities with basically unrestricted movement of the public, as well as the presence of drug abusers, trauma patients, distraught family members, and frustrated clients
- Low staffing levels at various times
- Isolated work situations during client examination or treatment
- One-person workstations in remote locations
- Lack of staff training relative to recognizing and managing escalating hostile and assaultive behavior
- Long waiting times for care in emergency areas, which can lead to patient frustration
- The increased presence in healthcare setting of gang members, alcohol and other drug abusers, trauma patients, and distraught family members
- Prevalence of handguns and other dangerous weapons

Other factors that contribute to workplace violence include stress, high patient-to-staff ratios, long working hours, and power and control issues of healthcare providers themselves.

Brockton Hospital in the suburbs south of Boston, MA, is considered a model for violence in healthcare. In 2007, OSHA investigated the hospital in response to complaints it had received and found that the types of physical assaults included, but were not limited to, punching, kicking, biting, scratching, and pulling hair. The agency recommended that the hospital analyze the workplace hazard, solicit extensive comments from employees, and develop a comprehensive violence-protection plan.<sup>12</sup> To date, this is the first and only hospital that OSHA has investigated as a result of the guidelines published in 1996 to prevent violence in the healthcare and social work settings. It should be noted that the OSHA guidelines (OSHA 3148) address only the violence inflicted by patients or clients against staff.

There are various ways of looking at violence in order to understand its impact on healthcare organizations. In this chapter, we will approach the subject from the basic categories of who, what, why, when, and where.

## The Who (Perpetrators/Visitors)

Those who are committing violence in emergency rooms are not typically gang members who are brought to the hospital after a violent confrontation with a rival gang and are looking for payback. Rather, it is citizens who are often intoxicated and upset with having to sit for hours in the waiting room.

There are four basic groups of perpetrators and victims in the healthcare environment: staff, patients, legitimate visitors, and illegitimate visitors. Figure 19-1 shows the many combinations of perpetrator to victim. The illegitimate visitor (trespasser/intruder) often is involved in stranger-to-stranger situations, while in the other groups, the perpetrator and victims are known. In the vast majority of past situations, both parties know each other, and their relationship has provided the motive for the violent act.

### Patients

We have previously discussed some situational events in both the outpatient and inpatient setting in which the perpetrator of violence is the patient himself. The clinical patient is often the source of confrontation, largely due to the volume of patients, long waits, and disputes relative to services being rendered. Hospital emergency departments, along with mental health evaluation and treatment areas, intensive care units, dedicated forensic patient care centers, and closed head injury units have historically the highest potential for violence. There are cases in which patients have attacked other patients or staff ostensibly without warning or provocation.

The Emergency Nurses Association, citing the US Bureau of Labor Statistics, revealed that 48% of all nonfatal assaults in the workplace are committed by healthcare

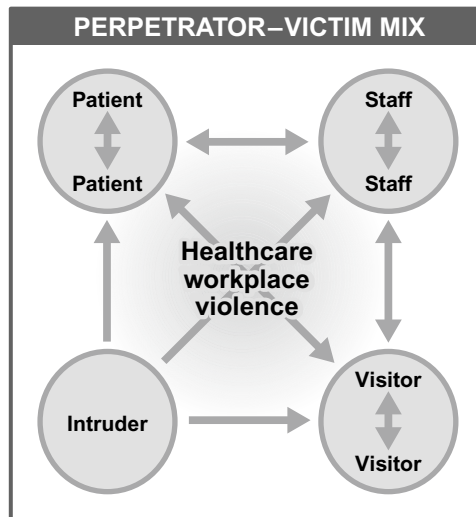


FIGURE 19-1 Healthcare workplace violence perpetrators and victims.

patients. Nurses and other healthcare workers suffer violent assaults at a rate 12 times higher than other industries.<sup>2</sup> Nurses are often on the receiving end of physical assaults, because they are typically the first and most frequent medical care providers by the bedside of ill and sometimes angry or frustrated patients. The ENA study showed that 86% of all emergency department nurses who responded to the survey had some form of violence committed against them while on duty over the past 3 years and one-fifth said they encountered it frequently. Much of the trend comes as more patients act out because of substance abuse or psychiatric problems. These patients have fewer treatment options following budget cuts at social service agencies. As such, the weapons used by the patient perpetrator to commit these violent acts are not knives, guns, or other weapons typically associated with violence in the community. Most often, the weapon of choice comes directly from the patient or the immediate environment. A listing of the most commonly used weapons by patients committing an act of violence is shown in [Table 19-2](#).

A study conducted by the University of Miami has found that 1 in 20 patients have had the urge to kill their physician. Distrust of physicians is believed to be the number one cause of the problem; however, there is still a lack of understanding who is likely to have a wish to harm medical staff and why. Further evidence-based research is needed to help reduce, mitigate, or even prevent these attacks. While few physicians are actually killed by patients, thousands are attacked and injured. Involvement in a disability compensation case is, for example, a predictor of a negative attitude, as patients often become angry if they feel their physician will not support their compensation claim.

Some care providers believe part of the problem of escalating violence is that some HCFs have made security officers less conspicuous in an effort to cultivate a friendlier, service-oriented setting. A more critical concern stems from the restrictions imposed by regulatory and accreditation agencies such as CMS and TJC that require healthcare organizations to apply medical restraints or seclude patients as a means of last resort. The pendulum of managing patient behavior is deemed at risk. There was a need to swing away from its previous position of being too prone to apply medical or chemical restraints or using seclusion rooms without the appropriate regard for patient safety. However, overly strict interpretations by surveyors and healthcare organizations alike have resulted in the compromise of employee, staff, and physician safety. Care providers are rarely using the tools available to them until after an actual incident of violence occurs. The result is more

**Table 19-2** Type of Weapons Commonly Used to Commit Violence in the Healthcare Environment<sup>13</sup>

Most Commonly Used Weapons	
<ul style="list-style-type: none"> <li>• Fists/hands/fingernails</li> <li>• Feet</li> <li>• Teeth/mouth</li> <li>• Head</li> <li>• Body fluids</li> </ul>	<ul style="list-style-type: none"> <li>• Medical supply/instrument</li> <li>• Food/utensils/meal tray</li> <li>• Furniture</li> <li>• Floor/door/wall/window</li> </ul>

incidents of violence and more injuries to healthcare workers and patients alike. To correct this vicious cycle, TJC, CMS, and healthcare organizations must take a more balanced approach in its interpretation of these patient restraint and seclusion guidelines before a safe and therapeutic healing environment can be created. If not, healthcare professionals will continue to leave their occupation because of the risk of actual and threat of violence, feeding the industry-wide shortage of qualified medical professionals.

## Visitors

There is a high potential for workplace violence caused by individuals or groups who are from outside the organization, which may include legitimate visitors such as patients' family members or illegitimate visitors. The illegitimate visitor is one who has no legitimate business being on the property. This type of visitor includes criminals contemplating or committing a crime (robbery, abduction, assault); gang members intent upon causing injury or harm; unwelcome friends or family members of staff or patients; protestors; terrorists; transient persons; and former patients and employees. It is almost impossible to discern the presence and intent of these persons until an overt act occurs. In fact, they often blend in with the legitimate patient, staff, or visitor.

The potential for violence from patients' family members has become a great concern for healthcare security professionals to address. The family who comes in after their loved one has been in a traumatic accident is under great stress with high anxiety levels. It can overwhelm their coping skills and be the cause of verbal abuse toward the care providers, front-desk receptionists, or other employees. However, violence against staff is not the only visitor concern.

Visitor violence against the patient is a troubling development that continues to plague the healthcare industry and threaten the reputation of many healthcare organizations that experience these often horrific events. At Baptist Hospital in Jackson, MS, a woman who was apparently overburdened with the stress of caring for her terminally ill mother killed her mother and then herself.<sup>14</sup> An isolated event for most hospitals, these types of violent episodes are not exceptional within the healthcare community.

In 2009, Rhonda Stewart got into an argument with her estranged husband in the Intensive Care Unit at Charleston Area Medical Center's Memorial Hospital in Charleston, WV. She was asked to leave by the hospital staff. She later returned with a gun and shot him in the head.<sup>15</sup>

In the parking garage at Baptist Medical Center in Jacksonville, FL, a 68-year-old husband pulled a gun and shot his wife and 11-year-old son as they were leaving the hospital and then shot himself.<sup>16</sup>

A Birmingham, AL, man was charged with attempted murder because he tried to drown his wife in a bathtub at Brookwood Medical Center where his wife was a patient.<sup>17</sup>

Untold healthcare organizations have had to manage the family member to patient cruelty associated with Munchausen by Proxy. Speaking at the 2009 IAHS Annual

General Membership Meeting and Seminar in Baltimore, MD, Sgt. Latrice Taylor from the University of Michigan Hospital in Ann Arbor shared two actual case studies that occurred at the facility within a 1-year span in 2008. Within the audience, 10–20% had experienced a similar event. *Munchausen by Proxy* is reviewed in greater detail in *Chapter 12, Patient Care Involvement*.

The legitimate visitor can also include outside service workers, construction workers, and vendors. While on occasion these people are responsible for violence, they do not present a major danger. Violence regarding these individuals is generally related to situational events occurring within the facility or in parking areas.

## Employees

Employees and staff members have been the source of many violent acts, especially against other employees or staff members. The day-to-day supervision, work evaluations, disciplinary actions, and terminations all set up situations that can be confrontational and that can provide the motivation of employee and ex-employee violence.

There is common agreement among human resource managers and security administrators that individuals who have committed violent acts in the past are potential perpetrators for further violence. Steve Millwee, CPP, author of *The Threat from Within: Workplace Violence*, is a leading authority on workplace violence and has found many similarities with employees prone to instigating workplace violence. [Table 19-3](#) lists many of the common characteristics and warning signs of the perpetrator of workplace violence.

A preventive approach to employee workplace violence requires recognizing that acting out may be the end result of an invisible process. No single characteristic or seemingly innocent experience can accurately predict violence. An individual may perceive that he or she has been unfairly treated, discriminated against, harassed, or purposely exposed to stress by a supervisor. Other mental factors such as stress, discrimination, and harassment can have a cumulative effect on the individual and lead to a traumatic event.<sup>19</sup>

**Table 19-3** Characteristics and Warning Signs of the Typical Workplace Violence Perpetrator<sup>18</sup>

Profile of the Workplace Violence Perpetrator	
<ul style="list-style-type: none"> <li>• Usually a loner; socially isolated without good support system</li> <li>• Long history of frustration and failure</li> <li>• Experienced some precipitating event, such as being fired or divorced</li> <li>• Difficulty handling defeat or rejection</li> <li>• Unusual fascination with weapons</li> <li>• Places blame for problems elsewhere; blames others for failure</li> </ul>	<ul style="list-style-type: none"> <li>• History of violence; made threats or acted out violently before</li> <li>• History of intimidating or threatening others; defiant, or blatantly violates organization procedures</li> <li>• History of illegal drug and/or alcohol abuse</li> <li>• Criminal history</li> </ul>

*Courtesy of Steven C. Millwee, CPP, SecurTest.*

The healthcare industry is not immune to these types of violent acts even if the media attention provided to these incidents is minimal. In November 2005, anesthesiologist Marc Daniel stabbed Lori Dupont, a nurse at Hôtel-Dieu Grace Hospital in Calgary, Alberta, and then killed himself. During a 3-month coroner's inquiry, the jury heard how the hospital allowed Daniel to continue practicing, despite complaints about Daniel's threatening behavior, such as breaking a nurse's finger and destroying hospital equipment, and Dupont's complaints that Daniel harassed her.<sup>20</sup>

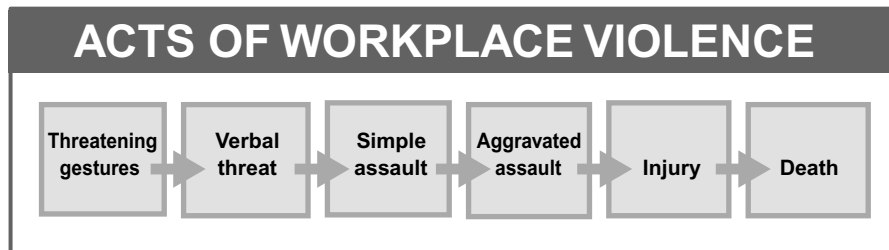
In April 2009, a hospital worker shot and killed two employees and killed himself at Long Beach Memorial Medical Center in Long Beach, CA.<sup>21</sup> Believed to have followed a recent downsizing, this event brought to life the importance of having an “active shooter” contingency plan as hospital workers were screaming and witnessed fleeing the facility in a panic. The active shooter and other security-related emergency contingency plans are discussed in greater detail in *Chapter 24, Emergency Preparedness—Planning and Management*.

## The What and the Why

The “what” of violence pertains to the specific act itself in terms of the severity or type of crime. The type of crime can be viewed on a continuum, as shown in [Figure 19-2](#).

There are at least three different categories of a violent act viewed from the causation or perpetrator viewpoint. These are the targeted victim, situational event, and the spontaneous event. The targeted victim is tied closely to stalking and generally involves a previous conflict between the perpetrator and the victim. The most common scenario in this regard is related to a domestic or intimate relationship. Violent acts in many of these cases are somewhat predictable, thus providing an opportunity to implement a number of possible prevention strategies.

The situational event generally results from a conflict between the perpetrator and the victim in the course of their interacting with each other. In the medical care setting, such conflicts often revolve around delivery of care issues. Patients may feel that they are not receiving the treatment they deserve or that their treatment is not timely. Sometimes it is not the patient but visitors who perpetrate the violence, whether it is at a hospital, clinic, physician's office, dentist's office, or long-term care facility. Violent acts resulting from such situational



**FIGURE 19-2** The acts of violence in the healthcare workplace.



conflicts are often fueled by drugs or alcohol. The mental health patient may be involved in confrontational situations that lack an apparent, or outward, rational motivation.

In spontaneous acts of violence, victims generally do not have a direct relationship with the perpetrators, and there is no forewarning of the danger. The act is premeditated and many have involved weeks, months, or years of planning or thought. The motive for these acts is usually general in nature and directed toward a cause, organization, or controversial issue. Unfortunately, the open healthcare environment is conducive to providing the opportunity for carrying out spontaneous violent acts.

One example of a spontaneous violent act occurred when a gun-wielding 57-year-old woman entered an eye clinic at the Henry Ford Hospital in Detroit, MI, and started shooting, severely wounding two technicians who she thought were physicians. Investigations revealed that she blamed physicians for the death of her mother, which had occurred over 4 years earlier. There was no evidence that she had previously complained of wrongdoing in her mother's death, had ever visited or been in Henry Ford Hospital, or had ever met the two technicians she shot.

## The When and the Where

Of course, there is no way to penetrate the minds of violent persons so that we can predict the time and location of an act. We do know that in the medical care setting, there are certain times and locations in which acts are more likely to occur. The most severe acts generally occur during the regular business day, when things are busy, facilities are open, and many potential victims are in close proximity to each other. For example, a disgruntled employee holding a grudge against the Human Resources office would not be able to act out his anger against department staff unless the office was open. On the other hand, employees and patients in the behavioral health unit and the emergency department are possible targets of violence 24 hours per day, 7 days a week.

While certain areas of the HCF present a higher risk than others for violence, no area can be considered immune. History has provided examples of violence in hospice units, admitting rooms, physician offices, stairwells, business offices, intensive care units, other patient care areas, cafeterias, materials management areas, and even in surgery areas. In the latter, an estranged husband shot and killed his former wife, a surgical technician, in the surgery area of a Louisville, KY, hospital. In Miami, FL, a hospice patient beat two nurses at a nurses' station so severely that both were hospitalized with serious injuries; neither returned to the career in nursing.

## The Management of Healthcare Violence

Not all violence occurring in the healthcare environment can be prevented; however, many acts can be prevented and managed to minimize injury, death, and damage to property. The three phases of managing violence in the workplace are before, during, and

after. The after phase provides information and lessons that help healthcare professionals to consistently improve preventive measures and intervention. The IAHSS has established a basic industry guideline to help healthcare organizations address the issues of violence in healthcare.

**IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.02**

**Violence in Healthcare**

**STATEMENT:** Healthcare facilities (HCFs) will implement an interdisciplinary protocol on workplace violence prevention and response.

**INTENT:**

- a. The protocol should elaborate on the five main components of an effective safety and security program, whose components also apply to preventing workplace violence:
  1. Management commitment and employee involvement
  2. Worksite analysis
  3. Hazard reduction and response
  4. Training
  5. Record keeping and program evaluation
- b. A multidisciplinary team should be appointed to develop and maintain the workplace violence program. The team should have express support of the facility's CEO along with authority for the program.
- c. Security staff should have a clearly defined role in the HCF's workplace violence program. Security often takes the lead role in coordinating the team. The team should receive orientation and training in evaluating and responding.
- d. Each HCF should establish a system such as patient record flags, electronic warning, chart tags, logbooks, or verbal census reports that identify patients and clients who may present assaultive or threatening behavioral challenges.
- e. Each HCF should establish policies and procedures prohibiting the carrying of firearms and other weapons onto the facility with the exception of authorized law enforcement officers, weapons carried by the facility's security officers, and others specifically authorized, such as armored care personnel.
- f. Each HCF is encouraged to post "No Weapons"-type signage at entrances to the facility.
- g. Each HCF should incorporate Targeted Violence protocols into its Violence in the Workplace policy or create a separate policy for preventing and responding to targeted violence (this would include domestic violence).

**REFERENCES/GENERAL INFORMATION:**

- Violence Occupation Hazards in Hospitals, DHSS (NIOSH) Publication No. 2002-101, April 2002.

- Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, U.S. Department of Labor Occupational Safety and Health Administration, OSHA 3148-01R, 2004.
- IAHS Targeted Violence Guideline 02.02.01.

**Approved:** January 2006

**Last Revised:** October 2008

## Preventive and Management Steps

There are three specific steps of preparation and response that organizations must implement to properly address workplace violence. The first step is to provide a reasonable level of security for the overall environment and especially to areas of probable conflict. This includes an organized security program that includes access control plans, proper physical security safeguards, enforced security policies and procedures, staff training and empowerment, and an effective critical incident response capability. To adequately plan and implement these essential elements, there must be strong commitment from top management and the board of directors to provide a high level of philosophical and management support. This support includes adequate funding of the protection program. Alan Butler, CHPA, a leading healthcare industry expert on violence prevention and mitigation, shares that effective workplace violence strategies include:

- Establishing a workplace violence prevention policy
- Establishing and maintaining security policies
- Examining and improving hiring practices
- Implementing prescreening techniques
- Conducting employee background investigations
- Encouraging employees to report threats or violent behavior
- Establishing termination policies
- Providing posttermination counseling
- Training all employees in the warning signs of aggressive or violent behavior
- Training management in threat assessment and de-escalation techniques
- Conducting formal workplace violence risk assessment
- Increasing security as needed
- Developing contingency plans
- Developing crisis and media communications plans
- Reviewing insurance coverage and verifying coverages and exclusions
- Identifying a defensive strategy

## The Threat Policy

The foundation of a successful violence prevention program is the organization threat policy, which is an everyday working document. The policy should state clearly that threats of any kind are not tolerated, that the staff is responsible for reporting all threats,

and should indicate the procedures for reporting such threats. In small organizations, the Human Resources department may be the central reporting point; in larger organizations, this may be the security department's responsibility. Regardless of size, there should be a central reporting department that has responsibility for initiating follow-up actions.

In very large organizations, there may be two or three different threat policies with some limited fragmentation for reporting and follow-up. For example, there may be a policy specifically for threats to employees and another one for threats to patients, visitors, and others. It is suggested that organizations preparing threat policies seek out such policies from other organizations as a valuable resource. In general, threat policies should include the following key points:

- Zero tolerance for threats against anyone on the property
- Mandated staff reporting of threats and reporting procedures
- Responsibility for immediate response and/or investigative action (24 hours per day)
- Staff obligation to report any application or knowledge of protective/restraining order naming the property of the organization as a protected area
- Statement of confidentiality of reporting party

## Response to Threats

The key to responding to violent events is having an effective system for recognizing, understanding, reacting to, and managing events as they develop and escalate.

There are two distinct types of threats in terms of response and follow-up action. The first type of threat is one in which time is of the essence and immediate response is required. The organization's critical response element should be empowered to take whatever steps are necessary to protect life and property in an immediate intervention. Take, for instance, the patient with a behavioral problem or a large group of loud and difficult visitors. The team leaders, e.g., lead physician, charge nurse, and security, can quickly huddle and decide whether to adjust the security response plan in anticipation of a potential problem.

In most situations of reported threats, there will be a window of time for planning, developing, and implementing the actions required. The degree and severity of the threat will be somewhat of a subjective judgment in terms of actions to be taken. All threats must be taken seriously. It is better to err on the side of taking too much action than doing too little too late.

### *Threat Response Team*

There should be a specific response team that evaluates and plans actions concerning all threats. The team should comprise the security administrator, director of Human Resources, nursing administrator, and in some cases the risk manager. The coordinator or leader of this team should initially decide the team member or combination of team members responsible for the management of the threat. A minor dispute between employees, resulting in a mild threat, might be handled by the director of Human

Resources and the affected department supervisor. In the case of a threat to a patient by a person outside the organization, there would possibly be a need to involve the entire team. In some emergency situations, a team member may immediately implement pre-conceived action protocols relative to the specific type of threat. A typical preconceived protocol may involve the domestic violence patient who has reason to believe that his or her assailant will come to the facility to cause further physical harm. Common steps in this regard may include:

1. Removing the patient's name from the list of inpatients (specifically from the switchboard and information desk and nursing station).
2. Assigning a room away from a stairwell.
3. Restricting patient visitation.
4. Changing room location so that the patient can be seen from the nursing station.
5. Using a private duty nurse.
6. Hiring a special security officer and/or requesting law enforcement services.

In extraordinary situations, the team would develop a specific plan for the situation. There should be a definite, identified authority for increasing, modifying, and ending the specific precautions implemented.

Another common threat that presents itself is the threatened staff member. These threats are often domestic-related and require preventative steps such as escorts to and from parking areas, work shift and/or location reassignment, restraining orders, or a change in work functions.

## Preventing Violence in the Workplace

All organizations need a strategy and plan to deal with workplace violence so that they can reduce the number of violent incidents and minimize the severity of these incidents to a large extent. The best means of managing workplace violence is to have a strong protection program in place that can be expanded to include specific facets of workplace violence. A program of preventing and managing workplace violence, in addition to a sound day-to-day security program, will include:

- A strong commitment from top management that preventive workplace violence is a priority both in terms of administrative and funding support
- Organization threat policy and procedures
- Staff training and education relative to staff responsibilities, early warning signs of escalating danger, de-escalation techniques, and general security awareness
- Encouraging employees to promptly report incidents and to suggest ways to mitigate or eliminate risk
- Reviewing workplace layout to find existing or potential hazards; installing and maintaining alarm systems and other security devices such as duress buttons or noise devices, cellular phones, and private channel radios where risk is apparent or

may be anticipated; and arranging for a reliable response system when an alarm is triggered

- The identification of criminal justice agencies, social agencies, and other community services as a resource to managing potential violent incidents
- Reporting of all incidents of violence
- Providing local law enforcement with floor plans of facilities to expedite emergency response or investigations
- The utilization of in-house resources such as employee health and employee assistance programs
- Setting up a system to use chart tags, logbooks, or other means to identify patients and clients with assaultive behavior problems
- Instituting a sign-in procedure with passes for visitors and compiling a list of “restricted visitors” for patients with a history of violence
- Proper screening of employee applicants
- Consistent enforcement of organization workplace rules and regulations including the facility access control policy
- Prosecution of perpetrators (serves as a deterrent and holds perpetrators accountable)

The NHS has put together a zero-tolerance initiative that requires trusts and health authorities to have systems in place for recording incidents of violence and aggression and to set targets for reducing the event of physical assaults against staff.

## Training

Fundamental to any workplace violence prevention strategy is conflict resolution training. However, no violence prevention education program is effective unless it gains employee involvement and support. There are many types of violence prevention and aggression management training programs. Ranging in length, some sessions are only an hour long, while other programs can extend to multiple full-length days. Some are lectures delivered by internal staff, while others are interactive programs conducted by outside contractors. Some new employees participate right away, others not until months (or years) after their hire. Only a few are tailored to the specific healthcare environment in which participants work. In short, there is little consistency in the conduct, content, and applicability of these programs, which are major contributing factors to their general ineffectiveness in violence prevention. However, all employees should receive training on the management of aggressive behavior and include physicians, volunteers, clerical staff, clergy, and contract employees of all job categories. By training together, staff members gain a better understanding of everyone’s role and develop a strong sense of teamwork, which will enhance communication and consistency in program administration. Medical staff will be more comfortable calling on security, for example, when they feel threatened or uncomfortable, and security will feel they are part of the patient care team.

Baystate Health, a three-hospital, multiple treatment center system in Massachusetts with nearly 10,000 employees, introduced new training for nurses, physicians, and care providers about how setting boundaries can be reconciled with customer service to help prevent workplace violence. The boundary-setting training teaches staff that it is okay not to share information or to say that while they are glad to be helpful, they do not have the requested information. Another major point is that customer service does not include accepting disrespect or aggression. If staff encounter abusive behavior, they are taught to express the desire to help but to be firm that the person asking for help must be respectful. The training also advises nurses to listen to their own bodily clues as a way to determine when a boundary needs to be set.<sup>22</sup>

Before they can recognize and respond to escalating tension in their work environment, however, healthcare staff must understand the basics of an effective response. Training should focus on evaluating each situation for possible violence when they enter a room or begin to deal with a patient or a visitor. If a violent situation is sensed, healthcare workers should never isolate themselves with the patient (or visitor). In these cases, staff should practice the concept of keeping an open exit pathway—never allowing a patient or visitor to stand between them and the door. If a situation cannot be diffused quickly, the care provider should be trained to remove himself/herself from the situation and call for assistance.

While there is no program that can train healthcare staff to handle every type of violent situation, most healthcare security administrators agree that it is possible to train them on the commonalities that occur in these situations. Most crisis intervention training programs include these lessons and help the employee look for physiological clues that an individual's aggressive behavior might escalate. Clues, for example, can be expressing anger and frustration verbally, nonverbal body language such as sweating or a lack of eye contact, or signs (smell) of alcohol or other drug use. Psychological skills needed by healthcare employees to manage conflict and aggressive situations include:

- *Understanding personal feelings about conflict.* Recognizing “triggers”; words or actions that immediately provoke an emotional response like anger.
- *Empathic listening.* Acknowledging the other person's feelings and going beyond hearing just words. Attempting to understand what is really being said by asking reflective questions, and using both silence and restatements. Not being judgmental of the individual's feelings. They are real—even if not based on reality—and must be attended to.
- *Generating options for resolving conflict.* Many people, even trained healthcare professionals, can think of only two ways to manage conflict—fighting or avoiding the problem. Working to resolve disagreements and discussing the pros, cons, and consequences are very useful tools. Matching threats or giving orders is discouraged.
- *Behaviors to avoid.* Shouting, sarcasm, power struggles, aggressive body language, profanity, degrading remarks, and disrespect. Violence and disrespect breed violence and disrespect. It is important to present in a nonthreatening, nonviolent manner

and avoid any behavior that may be interpreted as aggressive; for example, moving too fast, getting too close, touching, or speaking loudly.

- *Positive behavior and interaction techniques.* Intermittent eye contact, relaxed body posture and gestures, maintaining a calm demeanor, and listening. Maintaining a calm and caring attitude. The response will directly affect the individual.

As incidences of gang-related violence have increased, there has been an effort to teach healthcare professionals ways to avoid such conflicts. In 2006, the New Jersey Hospital Association teamed up with the New Jersey State Parole Board to develop a training program to teach hospital employees across the state how to recognize potential street gang affiliation through signs, colors, marking, and language. More than 20 hospitals across the state have taken advantage of the gang awareness program since its inception.<sup>23</sup>

Armed with that information, healthcare staff can build the confidence to take ownership in their role as a safety specialist as well as caregiver or caregiver support and work with other staff to manage the situation.

## Legislative Action

In 1995, the state of California introduced the Hospital Safety and Security Act (AB 508) to decrease the amount of violence being committed against hospital employees. The Act requires all acute care hospitals in California to conduct a security and safety assessment and to use the findings to develop a security plan with specific performance measures to protect personnel, patients, and visitors from aggressive or violent behavior. The plan includes specific security components such as<sup>24</sup>:

- Environmental controls to include physical layout and design, use of alarms and other physical security safeguards
- Staff-to-patient ratios
- Availability of security personnel who are trained in the identification and management of aggression and violence
- Specific violence prevention and response policies to include aggression and violent behavior management training
- Individual or committee responsibility for development of the security plan
- Reporting requirements

Hospitals in California are expected to track violent incidents that occur at the facility and analyze for trends as part of an annual quality-improvement process. In 2002, the University of Iowa's Injury Prevention and Research Center studied the hospital employee assault rates and violent events before and after the enactment of the AB508 and found the policy to be an effective method to increase the safety of healthcare workers.<sup>25</sup>

In 2009, the state of New Jersey introduced the "Violence Prevention in Health Care Facilities Act." Similar to AB 508 in California, the revised state statute requires hospitals, nursing homes licensed by the New Jersey Department of Health and Senior Services,



state and county psychiatric hospitals, and state-owned developmental centers to have in place a detailed, written violence prevention plan. The legislation declares that violence is an escalating problem in many healthcare settings in New Jersey and across the nation, and although violence is an increasing problem for many workers, healthcare workers are at a particular high risk.

The states of Washington and Tennessee have also developed similar legislation to help assure patients, visitors, and care providers of a reasonably safe and secure work environment.

## Prosecuting Perpetrators

Holding perpetrators of violence accountable for their action has become a focus of much attention from US and Canadian nurse and physician associations, the NHS, and many other entities. In 2008, tough new legislation was introduced in the United Kingdom, called the Criminal Justice and Immigration Act of 2008. In short, anyone causing actual violence in the healthcare setting could face fines of up to £1,000 and sentencing guidelines instruct judges that violence against care providers should lead to longer prison sentences.

The MNA introduced a bill that addresses the issue of workplace violence by increasing criminal penalties for those who commit assaults against care providers. The nurses association is ramping up a legislative campaign to criminalize assaults on healthcare workers in the line of duty—similar to a Massachusetts state law that protects ambulance crews, firefighters, and other public employees. It is also pushing a proposal that would require hospitals to identify factors that contribute to violent incidents and minimize them.

The West Virginia Hospital Association along with the state chapter of the American College of Emergency Physicians lobbied successfully to get the West Virginia Health Care Protection law into effect. The legislation places stiffer penalties on anyone who commits a violent act against any healthcare professional. The law applies to healthcare workers in hospitals as well as care providers in county or district health departments, long-term care facilities, physician offices and clinics, outpatient treatment facilities, and home health settings.

An ardent complaint of the Ontario Nurses Association with new legislation in Canada that requires employers to develop violence and harassment protocols and to take “reasonable precautions” to protect workers from domestic violence that may occur at work is that nothing in the legislation outlines punishment.

Orderlies at Perth’s (Australia) Sir Charles Gardiner Hospital organized a strike over the issue of violent patients, demanding better legal support and training to deal with violent situations. At the heart of the bargaining was better training to deal with aggressive and violent patient situations. At the time of the strike, the employees were provided only 2 hours in how to deal with and restrain violent patients.<sup>26</sup>

Figure 19-3 shows a sample language used in signs posted in patient rooms at a Jacksonville, FL, hospital.

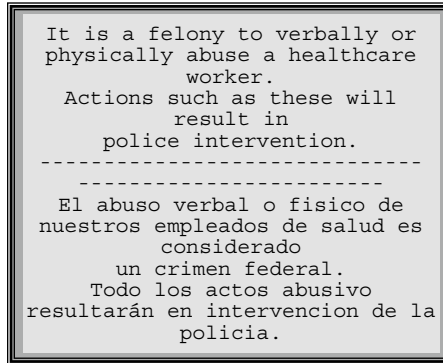


FIGURE 19-3 Sample violence signage language.

## Restraining Orders

In dealing with targeted victim situations, the utilization of court-ordered restraining orders is a fairly common safeguard. These orders may be available to the individual and to the organization. The restraining order has two specific purposes. One is to prohibit specific conduct by a specific individual and to order the individual to maintain a specific distance from the victim. In some cases, an organization may be able to obtain a restraining order without legal action. In these cases, the organization must prove that the conduct caused the individual to believe there was a threat of death or serious bodily injury. In all cases, a restraining order is only one element of managing a potential incident and should not be overly relied on in the course of business. Some of the most major crimes of workplace violence have been perpetrated by individuals who were under a restraining order. The IAHSS has established a basic healthcare industry guideline for addressing the issue of targeted violence.

### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.02.01

#### Targeted Violence

**STATEMENT:** Healthcare facilities (HCFs) will develop a policy and procedure to provide an appropriate response to manage targeted violence, through the provision of safety/security measures. Procedures are required to manage the risk of violence against a specific target, usually an individual, individuals, or group and should include a threat assessment component.

#### INTENT:

- a. Definition: Targeted Violence—a situation where an individual, individuals, or group are identified at risk of violence, usually from another specific individual such as in cases involving domestic violence. Often the perpetrator and target are known prior to an incident.

- b. The three major functions of a threat assessment program are identification of a potential perpetrator, assessment of the risks of violence posed by a given perpetrator at a given time, and management of both the subject and the risks that he or she presents to a given target.
- c. The HCF policy should identify responsibility of staff to report a risk of targeted violence as quickly as possible so that the threat can be assessed and preventative measures can be initiated as required.
- d. Mechanisms should be in place to encourage reporting of threats where personal safety may be at risk.
- e. All identified threats of targeted violence will be treated seriously and assessed through a process that analyzes the threat and recommends the appropriate level or type of intervention to be initiated.
- f. Security should play a lead role in the threat assessment process and design of any required safety plan. Security staff should be fully informed of all targeted violence situations and have a defined role in the procedure.
- g. HCF staff involved in the process of assessing the threat to determine the appropriate level and type of intervention required should receive training for this role.
- h. Where warranted by risk in specific circumstances, HCFs should employ preventative measures to protect the potential target. Measures could include:
  1. If a patient, no information/privacy block on patient information system or, if a worker, protecting information related to work location.
  2. Communicating with security to provide information.
  3. Information to be shared with workers or other individuals in the area as appropriate.
  4. Involvement of staff or family members for support as necessary.
  5. Consideration of moving the person at risk to another care area or another site.
  6. Restriction on visitors or access to the potential target, including lockdown of the area if required.
  7. In appropriate circumstances, notify law enforcement.
  8. Document risk and preventative measures initiated. These measures should be considered, in sum or in part, on the basis of specific circumstances. The level of threat will determine the scope and timing of the response.
- i. The safety of the potential victim will be of paramount concern at all times.

**REFERENCES/GENERAL INFORMATION:**

- IAHSS Guideline 02.02, Violence in Healthcare.
- Canada, Department of Justice, “Criminal Harassment: A Handbook for Police and Crown Prosecutors.”
- IAHSS, U.S. Department of Justice, National Institute of Justice, “Threat Assessment: An Approach to Prevent Targeted Violence.”

**Approved:** July 2008

**Last Revised:** October 2008

## References

1. *The USDA Handbook on Workplace Violence Prevention and Response*. (1998, December). The U.S. Department of Agriculture. Retrieved June 13, 2009 from <http://www.usda.gov/news/pubs/violence/wpv.htm>.
2. Emergency Nurses Association. *2007 Study of Workplace Violence Against Registered Nurses in Emergency Departments*. Retrieved June 8, 2008 from <http://www.ena.org/research/current>.
3. University of Michigan Health System. (2005, February 15). Majority of emergency physicians report experiencing at least one violent act a year. Retrieved September 9, 2007 from <http://www.med.umich.edu/opm/newspage/2005/edviolence.htm>.
4. Massachusetts Nurses Association. (2008, October 22–24). International Conference on Workplace Violence in the Health Sector. De Meervaart, Amsterdam, Netherlands. *Workplace Violence Prevention at the MNA*. Retrieved June 16, 2009 from <http://www.massnurses.org/health-and-safety/workplace-violence/workplace-violence>.
5. Turner, J. T. (1984). *Violence in the medical setting: A survival guide*. Rockville, MD: Aspen Systems Corporation.
6. Heskett, S. L. (1996). *Workplace violence: Before, during, and after*. Boston, MA: Butterworth-Heinemann.
7. Marston, C. (2008, April 13). Violence part of life for NHS staff. *BBC News*. Retrieved April 13, 2008 from <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/health/7337389.stm>.
8. Mulholland, A. (2009, April 25). Nurses say they are fed up with workplace violence. *CTV.ca News*. Retrieved April 29, 2009 from [http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20090416/nurses\\_090425/20090425?hub=TopStories](http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20090416/nurses_090425/20090425?hub=TopStories).
9. Ironside, R. (2008, December 22). Fed-up Queensland nurses turning to prostitution. *The Courier-Mail*. Retrieved December 22, 2008 from <http://www.news.com.au/story/0,27574,24831036-1248,00.html>.
10. Lazar, K. (2008, November 11). Violence in ER a growing problem. *The Boston Globe*. Retrieved November 12, 2009 from [http://www.boston.com/news/local/articles/2008/11/11/violence\\_in\\_er\\_a\\_growing\\_problem/?page=2](http://www.boston.com/news/local/articles/2008/11/11/violence_in_er_a_growing_problem/?page=2).
11. National Institute of Occupational Safety and Health. (1996, July 16). *Violence in the workplace*. Retrieved December 22, 2008 <http://www.cdc.gov/niosh/violintr.html>.
12. Valencia, M. J. (2007, August 21). Hospital urged to protect against violence. *The Boston Globe*. Retrieved August 23, 2007 from [http://www.boston.com/news/local/articles/2007/08/21/hospital\\_urged\\_to\\_protect\\_against\\_violence](http://www.boston.com/news/local/articles/2007/08/21/hospital_urged_to_protect_against_violence).
13. Peek-Asa, C., PhD, et al. *Workplace Violence and Prevention in New Jersey Hospital Emergency Departments*. National Institute for Occupational Safety and Health. Retrieved June 29, 2009 from [http://pdcbank.state.nj.us/health/surv/documents/njhospsec\\_rpt.pdf](http://pdcbank.state.nj.us/health/surv/documents/njhospsec_rpt.pdf).
14. Woman fatally shoots mom, self at hospital. (2007, September 29). WLBT3. Retrieved October 8, 2007 from <http://www.wlbt.com/global/story.asp?s=7147686&ClientType=Printable>.
15. Rivard, R. (2009, June 16). Many hospitals seeing increase in violence. *Charleston Daily Mail*. Retrieved June 16, 2009 from <http://www.dailymail.com/News/200906150690>.
16. Woman shot at hospital dies; son recovering. (2008, June 20). *News4Jax.com*. Retrieved June 21, 2008 from <http://www.news4jax.com/print/16663671/detail.html>.

17. Bryan, K. (2008, March 26). Man tried to drown wife in hospital tub. *The Birmingham News*. Retrieved March 30, 2008 from [http://blog.al.com/spotnews/2008/03/man\\_tried\\_to\\_drown\\_wife\\_in\\_hos.html](http://blog.al.com/spotnews/2008/03/man_tried_to_drown_wife_in_hos.html).
18. Millwee, S. C. (2003). *Firing the Violent or Threatening Employee Without Being Fired On*. SecurTest, Inc. Retrieved June 30, 2009 from [http://www.safetampabay.org/publications/WPViolence\\_2003.pdf](http://www.safetampabay.org/publications/WPViolence_2003.pdf).
19. Lindsey, D. (1994). Of sound mind? Evaluating the workforce. *Security Management*, 69.
20. A killing at Hotel-Dieu: Murder suicide shocked the community. (2006, November 4). *The Windsor Star*. Accessed June 14, 2009 from <http://www2.canada.com/windsorstar/features/dupont/features/dupont/story.html?id=c79312d5-a2c7-43e8-a274-30f2e8ec1b1d>.
21. Taxin, A. (2009, April 16). Police: 3 dead in California hospital shooting. *The Associated Press*. Retrieved April 22, 2009 from <http://www.foxnews.com/story/0,2933,516888,00.html>.
22. Longmore-Etheridge, A. (2007). Nurses on guard. *Security Management*, 55–56.
23. Thompson, L. E. (2009, February 23). New Jersey hospitals gang up on ED violence. *Nurse.com*. Retrieved February 24, 2009 from <http://news.nurse.com/apps/pbcs.dll/article?AID=2009302230056>.
24. State of California. *California Health and Safety Code Section 1257.7*. Retrieved June 29, 2009 from <http://law.onecle.com/california/health/1257.7.html>.
25. Casteel, C., Peek-Asa, C., Nocera, M. (2009). Hospital employee assault rates before and after enactment of the California Hospital Safety and Security Act. *Annals of Epidemiology*, 19(2), 125–133.
26. Hospital orderlies strike over violent patients. (2007, December 10). *Australian Broadcasting Channel News*. Retrieved December 11, 2007 from <http://www.abc.net.au/news/stories/2007/12/10/2114306.htm>.

# Security Sensitive Areas

The term *security sensitive area* was coined by TJC relative to their standards and elements of performance. The security sensitive area pertains exclusively to the protection arena. While non-TJC-accredited facilities are not bound by commission requirements, the commission requirements provide all organizations with a logical and practical method of identifying and approaching certain basic protection issues for areas of highest risk.

There is a clear distinction between the security sensitive area and the area that may have special security concerns. All healthcare organizations will identify certain risks in their respective environments that require enhanced or special security safeguards. It is the responsibility of the organization to make the decision, through the security risk analysis process, as to which areas have exceptional risk, rendering them security sensitive areas or lower risk areas of special concern. Common areas of special security concern are discussed in *Chapter 21, Areas of Special Concern*.

## Security Sensitive Areas

For our purposes, it is helpful to view security sensitive areas in two categories. The first category involves the vulnerability to persons, such as in the birthing unit, the mental health unit, remote parking areas, the emergency clinical care area, and perhaps even the intensive care unit. The second category involves property. Areas that may be included in the property category are the pharmacy, medical records, information services, research labs, and cashier areas. In those cases, it is the product or function that sets up the potential for a dangerous situation. For example, the drugs in the pharmacy create a higher risk of armed robbery, yet the dollar loss potential to the organization is quite low. The operation of an animal research lab, on the other hand, sets up the potential for high dollar loss in relation to information and property damage as opposed to high exposure to staff injury.

The TJC has not issued a clear and precise definition for their term security sensitive area. In this discussion, the term will be defined as a location whose function or activity presents an environment in which there is a significant potential for injury, abduction, or security loss that would most likely severely impact the ability of the organization rendering a high quality of patient care. This is often based on the potential for violence or use

of weapons, especially vulnerable populations such as the elderly, infants, and children, and the availability of drugs or cash handling areas. The IAHS has a specific security industry guideline to guide healthcare facilities (HCFs) in the identification and protection of security sensitive areas.

#### IAHS—HEALTHCARE BASIC SECURITY GUIDELINE, #09.01

##### **Security Sensitive Areas**

**STATEMENT:** Healthcare facilities (HCFs) will identify security sensitive areas during security risk assessments. The objective of the security risk assessment is to identify security sensitive areas and to develop reasonable measures to minimize vulnerabilities.

##### **INTENT:**

- a. Common security sensitive areas for HCFs include the following: EDs; pharmacies; mental health units; infant and pediatric areas; laboratories; specialized treatment clinics (e.g., substance abuse, abortion); surgery; ICUs; and plant services. Security sensitive areas are those in which the mere existence of a particular function or material is, in and of itself, a primary risk factor.
- b. The senior manager of such sensitive areas should be involved in security planning.
- c. The HCF should develop a security plan for each security sensitive area. Where appropriate, the plan should include the following:
  1. Security conditions unique to the identified area;
  2. Control of entry to and exit from the area;
  3. Identification of visitors, patients, staff, and other people entering the area;
  4. Electronic security components to include CCTV, alarm monitoring, or other devices for the designated area;
  5. Maintenance procedure for reducing the potential for system failures of panic alarms, cameras, etc. should be developed including periodic testing procedures;
  6. Security training for staff members and, as appropriate, for families and patients;
  7. A security incident response plan for the area.

**Approved:** December 2006

**Last Revised:** October 2008

There are three major areas of healthcare that would normally involve the designation of security sensitive area: the ED, the infant care/birth center, and the pharmacy. Other areas in specific healthcare delivery systems may require the organization to designate additional security sensitive areas. These include pediatric units, specialty clinics (such as methadone, detoxification, or abortion), research labs, mental health units, and centralized information departments.

Each TJC-accredited hospital organization must designate their security sensitive areas in their security management plan. When the declaration is made, there are three

basic security components that must be developed and implemented relative to the security sensitive area. These components are a specific security access control plan for the area; security orientation and education specific to area risks, which minimizes the danger to staff, patients, and visitors; and a critical incident response plan.

## Area Access Control Plan

The security sensitive area must have a written plan to control or regulate access including how nonemployees are screened, identified, and directed to service points specific to the area. Building on the overall facility access control plan, the healthcare organization should not limit its discussion of access control to just locks and keys. It can consist of staff-assigned responsibilities, identification systems, as well as the various physical safeguards that may be appropriate.

The level of access control and restrictions employed may vary from facility to facility. Determining what restrictions should be employed is best determined as part of the annual assessment of security sensitive processes, a newly revised TJC requirement introduced in 2009.

## Staff Security Orientation and Education

Every staff member who works in the security sensitive area must undergo specific security training. This training includes understanding the processes and staff contributions for the protection of the area, how to identify potential security compromises, how to minimize security risks for all persons within the area, and how to react to specific breaches of security. How this is accomplished is not prescribed by TJC. Common methodologies include:

- Initially training new employees about their roles in the access control and critical incident response plans
- Periodically conducting drills to test the response to a critical incident, correcting weaknesses in the plan and/or retraining staff, and documenting all such activities
- Annually retraining all employees about their roles in the access control and critical incident response plans

## Critical Incident Response Plan

Each security sensitive area must have a specific critical incident response plan. This written plan should describe the unit employee response to the primary security threat of the area. It should include how employees respond to predetermined events that negatively impact department performance and/or personal security (usually those events that caused the area to be declared security sensitive). The plan must be activated immediately when the preventive steps of access control and staff actions have failed to prevent a major security incident. This plan will generally be formulated for unit staff reaction, while more general and organization-wide response plans will be generated by security.



An example of this concept can be viewed in the infant birthing unit. The plan for this unit would be prepared by the unit manager and focus on the abduction of the newborn. Input and collaboration with the security department would of course be part of the methodology in developing the plan. There is also the possibility of other major incidents occurring in the birthing unit, such as hostage taking, bomb threats, or serious assaults, which are not unique to the birthing unit itself. The formulation of the critical incident response plan for these events would be the responsibility of the security department in collaboration with various facility staff and/or departments.

The responsibility for the preparation of the security sensitive area critical incident response plan rests with the unit manager in collaboration with the healthcare security administrator. The plan will almost always involve actions of various facility departments and staff and thus is not limited to just the actions of the unit staff or security. In the case of an infant abduction, the response is required of every employee in the healthcare organization.

In this chapter, the three primary security sensitive areas—the infant birthing area, the ED, and the pharmacy—will be discussed; however, this should not infer that these are the only three areas for facility consideration. Each facility will have specific functions or areas that present major security threats.

## Infant Abductions from HCFs

The abduction of an infant from an HCF is an event that generates a considerable amount of media attention. Newspapers, magazines, and TV talk shows have addressed the various aspects of infant abduction so that the risk is now widely recognized. However, in recent years, the number of nonfamily infant (from birth to 6 months) abductions from hospitals has been drastically reduced. This reduction is due, in large part, to the efforts of the National Center for Missing and Exploited Children (NCMEC). It was not until 1987, when the NCMEC studied the problem of US infant abductions, that the extent of these incidents was known. Their study data date back to 1983 and their research and tracking continue as an ongoing NCMEC program. In particular, the work of John Rabun, Vice President and Chief Operating Officer, Cathy Nahirny, Senior Analyst/Supervisor, and the highly dedicated staff of the NCMEC have truly made a difference.

The NCMEC does not just study the problem; it also provides ongoing training and education and is an instant resource to facilities and law enforcement agencies when an abduction occurs. The work of the NCMEC goes far beyond hospital infant abductions; however, the majority of this discussion focuses on nonfamily abductions within the healthcare delivery system.

The delivery system involves over 4.3 million births each year in approximately 3,500 US birthing facilities and continues to a limited degree after discharge. Hospital-operated or independent home healthcare agencies frequently provide aftercare to the mother and baby in the home. The healthcare security administrator must also be aware that there can be a certain degree of organizational responsibility for infant safety

in the home after discharge from the hospital. In the event that information, action, or inaction on the part of the healthcare organization caused or contributed to a criminal act in the home, there could be certain legal ramifications.

In 1989, the NCMEC issued its first set of guidelines relative to the abduction of the newborn, entitled *For Hospital Professionals: Guidelines on Preventing Abduction of Infants from the Hospital*. The most current NCMEC guideline (9th edition) was released in January 2009 and is titled *For Healthcare Professionals: Guidelines on the Prevention of and Response to Infant Abductions*. This publication goes beyond safety in the maternal-childcare unit to safety in special care nurseries, pediatric facilities, outpatient areas, and the home.<sup>1</sup>

The number of infants abducted from hospitals (from 1983 to June 2009), including the location of the abduction and degree of violence, is shown in [Table 20-1](#). The number of infant abductions from hospitals and homes by state (includes Puerto Rico and the District of Columbia) for the same period of time is shown in [Table 20-2](#).

In addition to the NCMEC guidelines for preventing infant abductions, several states have enacted legislation mandating hospitals to implement certain infant security measures.

Statistically, the risk of an actual abduction is low. However, statistical relevance is not important to the family that is the victim of an abduction, the healthcare organization's staff, or the HCF. This event is devastating and takes an emotional and physical toll on all involved. The organization's reputation for safe patient care may suffer as well even if the organization does everything appropriate to avoid abduction.

**Table 20-1** Infants (under 6 Months) Abducted by Nonfamily Members from US Healthcare Facilities, from 1983 to June 2009

Abducted From	Number	Percent
Mother's room	72	57
Nursery	17	14
Pediatrics	17	14
On premises	20	16
TOTAL	126	100
Outcome		
Recovered	119	94
Still missing	7	6
TOTAL	126	100
Violence to mother	9	7

Courtesy National Center for Missing and Exploited Children, Alexandria, Virginia.

**Table 20-2** The Number of Infant Abductions from US Hospitals and Homes, by State, from 1983 to June 2009

State	# Cases	State	# Cases
Alabama	3	Montana	1
Arkansas	3	Nevada	1
Arizona	4	New Hampshire	1
California	34	New Jersey	6
Colorado	6	New Mexico	4
Connecticut	2	New York	10
District of Columbia	6	North Carolina	4
Delaware	1	Ohio	10
Florida	20	Oklahoma	4
Georgia	9	Oregon	3
Illinois	16	Pennsylvania	8
Indiana	2	Puerto Rico	4
Iowa	1	Rhode Island	1
Kansas	3	South Carolina	5
Kentucky	3	South Dakota	1
Maine	1	Tennessee	5
Maryland	10	Texas	33
Massachusetts	2	Utah	2
Michigan	6	Virginia	8
Minnesota	1	Washington	4
Mississippi	3	West Virginia	1
Missouri	7	Wisconsin	2

*Courtesy National Center for Missing and Exploited Children, Alexandria, Virginia. Note: States that are not listed in this table have not reported an abduction by a nonfamily member from a hospital or the home during this time period (26 years).*

The number of infant or pediatric abductions from hospitals by family members is not known. These cases, which are generally based on custody issues, are not tracked by any central tracking organization. Likewise, the number of attempted infant abductions from hospitals is not known. Anecdotal evidence suggests that there are many more abduction attempts each year than reported. However, circumstances surrounding possible abductions that do not occur would be speculative at best.

The areas of greatest risk for infant and child abductions include the mother's room, nursery, postpartum units, pediatric care areas, and neonatal intensive care units as well as well-baby units. But because these units may present more of a challenge to anyone

trying to abduct an infant, an abductor may try to get a child in waiting areas for hospital clinics, radiology, and the ED. Child development centers on the HCF may also become a target.<sup>2</sup>

## Hospital Infant Environment

Since the early 1980s, there has been a relaxed environment in the delivery and care of infants in hospitals. Family members are now allowed to view the delivery process and are freely admitted to nurseries. Visitor restrictions have also been relaxed to permit greater family involvement; the crowds in some birthing rooms resemble a small family reunion.

Baby viewing areas are considered quasi-public areas, and hospitals are in some sense inviting people in to view the infants. It is one place in a hospital that is upbeat, friendly, and warm. Hospital inpatients and family members often visit this area, and it can be good therapy for many.

The new relaxed environment does not mean, however, that security safeguards should be relaxed. With the greater number of people involved, security must be strengthened, maintained, and constantly evaluated.

## Profiling the Typical Abductor

Research of the NCMEC has enabled them to build a profile of the typical infant abductor produced from those who have abducted infants from hospitals. These are the general characteristics of the abductor:

- Females of childbearing age (range 12–50 years old)
- Usually lives in the community where the abduction takes place
- Low self-esteem, emotionally immature, compulsive, and manipulative
- Is in a relationship (either married or cohabitating) that is on the verge of collapse
- Usually no previous criminal record

In many cases, the abductor has convinced others that she is pregnant. The abduction occurs during the alleged ninth month when the woman must produce a baby at all costs.

Analysis of the 126 cases yields some other interesting information. The abductor will most likely take an infant whose skin color matches her significant other's to ensure he will accept the infant presented to him as his baby. The NCMEC has also found that many non-English-speaking mothers are victimized by bilingual abductors who are able to portray themselves as different things to different people. To a victim mother, the abductor may present herself as a member of the hospital staff while at the same time presenting herself to the hospital staff as a member of the mother's family.

### *Abductor Modus Operandi*

The abductor will often use common methods during the abduction, including:

- Indicating to others that she has “lost” a baby or may be incapable of childbirth
- Planning the abduction, but not targeting a specific infant (except possibly race)

- Visiting multiple birthing facilities in the community, seeking an opportunity to carry out the abduction —“window shopping”
- Impersonating a clinical provider or other healthcare person
- Spending time becoming familiar with healthcare personnel and befriending the infant’s parents
- Demonstrating the desire and capability of providing good or appropriate care to the infant after the abduction

## The Basics of the Infant Security Plan

The basics of providing infant security are identification (mom, baby, significant other, and the caregiver staff), education (mom and staff), and physical and electronic security safeguards. These three elements of infant security intertwine with the critical incident response plan to provide the desired level of access control and infant safety. The IAHSS has developed a basic security industry guideline for HCFs to deter and respond to infant/child abductions.

### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #09.02

#### **Infant/Pediatric Security**

**STATEMENT:** Healthcare facilities (HCFs) providing medical services for infants and children will develop a program to deter the abduction of an infant or child as well as procedures to respond to an abduction incident.

#### **INTENT:**

- a. The program will be based on identified risks at the HCF as well as current professional literature on infant/child abduction.
- b. The program will include policies, procedures, and protocols to deter infant/child abduction and to respond to suspected or actual abduction for both nonfamily- and family-related abduction incidents.
- c. The program will include training of multidisciplinary healthcare staff in both deterring and responding to abductions.
- d. The program will include the use of physical and electronic security measures, based on the HCF’s ongoing risk assessment.
- e. The use of the words “CODE PINK” to institute a response to an infant/child abduction or suspected abduction is encouraged. In the United States, the words “Code Pink” are commonly used to institute a response to an infant/child abduction or suspected abduction. Internationally another code may be in use.
- f. Abduction drills should be conducted to the HCF abduction response plan.

**REFERENCES/GENERAL INFORMATION:**

- National Center for Missing and Exploited Children (NCMEC) publication “For Healthcare Professionals: Guidelines on Prevention of and Response to Infant Abductions,” Ninth Edition—2009. NCMEC, 699 Prince Street, Alexandria, VA 22314-3175
- JCAHO Sentinel Event Alert, 4/9/99
- TJC Current Standards, Rationale, and Elements of Performance

**Approved:** December 2006

**Last Revised:** October 2008

## Identification

The most commonly utilized method of visual identification of the infant is the four-band (bracelet) system. These four identical bands link mom, baby, and significant other. The infant is banded on the wrist and ankle, while the mom and significant other wear similar bands on their wrists. However, infant identification goes far beyond bracelets. It is a combination of elements that should be viewed as a package, each complementing and supporting the other. Each element of the infant identification package must be completed prior to the removal of the baby from the birthing room and in all cases, within 2 hours of birth. The elements of identification are:

- *Footprints.* The footprint is an excellent form of identification if an infant is abducted and recovered even months later.
- *Color photograph.* Digital cameras are a popular method of achieving this element of identification as it can instantly become part of the infant’s medical record. Other types of cameras can be utilized, although the requirement is that the photograph must be taken within 2 hours of birth.
- *Full physical assessment.* The physical assessment of the infant must record any marks or abnormalities.
- *Cord blood.* A sample of cord blood for future identification typing should be taken and retained until 24 hours after the infant is discharged from the facility.

An additional method of identification is antibody profiling. Mother and baby share the same antibody profile for the first year. Unlike DNA testing, which can take up to 2 weeks to get results, the antibody profile can be performed within hours. Such antibody profiling is most useful in resolving any question as to the mix-up of babies and mothers.

A number of hospitals have prepared an attractive baby record “kit” that is provided to the parents at the birth of their infant. This kit is a duplicate of the footprint, photograph, and physical assessment that was completed for the infant’s medical record.

The visual identification of hospital staff is a key element of the infant security plan. Each staff member who is authorized to be transporting or maintaining control of

the infant must wear a unique form of identification. This identification must differ, in a noticeable way, from regular hospital identification. This identification, most often a photo identification badge, must be worn above the waist and in a manner that is visible to mother and other staff at all times. A common method in developing the unique badge is to utilize a different color background for either the staff person's photograph or for the background of the badge itself.

This special badge is generally issued permanently to regular staff; however, there must be a system for the issuing of a temporary badge on a shift-to-shift basis. The temporary badge is utilized when temporary staff or students are participating in infant care and when a regular staff member does not have their regularly issued badge in their possession for a variety of reasons. These temporary badges must be tightly controlled with a method of strict accountability. Many healthcare organizations use the narcotics dispensary machine on the unit to issue and maintain an audit trail for the temporary badges. On termination of the regular mother/infant caregiver, there must be a diligent effort to retrieve and destroy the identification badge. In addition, a new regular baby staff identification badge should be developed at least every 5 years and whenever there is a significant security compromise involving the badge identification system.

## Prevention Through Education

Education is critical to preventing infant abductions from healthcare facilities, and that means educating both staff and parents. NCMEC's publication *For Healthcare Professionals: Guidelines on the Prevention of and Response to Infant Abductions* contains detailed information for healthcare staff, including nursing guidelines and security guidelines. It also has information for patients, including a chapter titled *What Parents Need to Know*.

### *Staff Education*

There must be continuous education and training of the caregiver staff as they are the first line of defense. Unit staff members should wear a unique form of identification and demonstrate an awareness of the importance of this special security practice relative to the protection efforts employed. Training should begin with basic training in customer service. Greeting everyone who comes on the unit has an immeasurable deterrent value and is a good security practice. In the majority of infant abductions, there have been one or more observations by staff that, properly followed up, would have prevented the abduction. When a situation does not quite look right or if there are unidentified persons on the unit, staff must act to investigate and clarify the situation or determine the legitimacy of the unknown person. A March 2009 thwarted infant abduction at South Jersey Healthcare Regional Medical Center in Vineland, NJ, is credited to an alert unit secretary who realized that the abductor, dressed in scrubs, wearing an ID badge, and identifying herself as a midwife, was an imposter.<sup>3</sup> Unit staff awareness and alertness is believed to be one of the most critical elements of the infant security plan. When exercising the infant security plan, almost every mock abductor shares that his/her greatest fear of carrying out the plan is being approached by a unit staff member. When it occurs, it is very

**Table 20-3** Staff Training Considerations on Infant Security**Infant Security Training for Healthcare Staff**

- The profile of an infant abductor
- Commons methods of operation for the typical abductor
- Importance of being alert to unusual behavior
- Role in critical incident response plan (Code Pink)
- Guidelines for what parents need to know to include providing continuous parental education
- Restricting access to hospital materials (uniforms and other means of identification)
- Overview of prevention measures used (wearing unique form of identification, video surveillance, access control, infant tagging, etc.)
- Common diversionary techniques (fire alarms, disturbances in waiting areas, Code Blue activations, etc.)
- How to answer questions about infant security (in person and by telephone)

disruptive as anxiety levels rise and confidence in being able to carry out the abduction is lost, hardening the organization as a target. [Table 20-3](#) lists other important staff training considerations that all staff members should be exposed to. In addition, a semiannual review of the infant security plan should be completed on a formal basis with all staff members. All training should be documented.

Mead Johnson Nutritionals, working in conjunction with NCMEC, has developed a free training video for healthcare professionals called *Safeguard Their Tomorrows*, which has been distributed to hospitals nationwide since 1991. This program was revised for the third time in 2009 and has provided education and training on infant security to thousands of healthcare providers, security, and law enforcement since its first release. To further enhance training efforts, healthcare security administrators are encouraged to periodically quiz noninfant care staff members on their duties during a potential infant abduction. This should include what hospital staff members are expected to do if “they find the person they are looking for.” Infant abduction drills are useful training tools to further test staff members by having the “mock abductor” scouting the unit prior to the drill and calling the hospital to learn what staff will share about the protection measures in place.

### *Parental Education*

Evidence collected by NCMEC provides that an overwhelming 56% of all infant abductions occur from the mother’s room. As such, the role of parental education is a critical yet often overlooked element of the infant security plan. Unfortunately, it is an area not easily tested with infant abduction drills and other exercises.

The proper education of mothers is crucial to the infant security system. This education often begins in prenatal classes and continues to some degree until discharge, and includes after discharge care at home. The NCMEC has developed a checklist, entitled *What Parents Need to Know*, which contains sound parenting techniques that bear directly on the safety and security of the new infant. This checklist is contained in the guidelines document previously referred to. Distributed to prospective and new parents, the *What*



*Parents Need to Know* information can be strategically posted on the birthing unit and in each patient bathroom.

When parents are educated is a concern. In most HCFs, it is conducted as part of the prenatal education classes offered by the hospital. Upon admission to the hospital, the mother is often fully briefed concerning the security procedures. Unfortunately, for most new mothers and fathers, the timing of when parents are educated on their infant's security is off the mark. The concern of most new mothers and fathers during these two periods is on having a successful childbirth and they rarely focus on anything else. In addition to preadmission and admission education, it is important to remind mothers and others of the importance of security during the entire (even though it may be a very short) stay with postings and a few key reminders. It is strongly recommended that there be a briefing form signed by the soon-to-be mom. This form should become a component of the mother's medical record. See [Figure 20-1](#) for an example of a briefing form.

Unit staff should play an important role by providing information to parents on whom they should release their infant to. An excellent shift-change protocol for the assigned care provider at the beginning of each shift is to remind mom of the importance of the unique form of identification worn by staff. Instituting a standard practice of informing *mom* of everyone who will be coming in for testing, etc. is a simple yet effective tool to combat the potential abductor who attempts to fool the mother into willingly handing over her baby. Organizations with separated labor and delivery from postpartum have an excellent opportunity to remind mom of her role and responsibility for her infant's security during her transfer from the labor and delivery unit to postpartum unit. Message stickers on the room mirrors and bedside/dresser table tents are frequently used. Iowa Methodist Medical Center in Des Moines has developed a security education poster that is placed on the back of the bathroom door, as shown in [Figure 20-2](#).

The facility should be very clear as to whether there will be any home care provided or home visits by hospital staff. To date, the abduction of an infant from the HCF has not entailed violence; however, there is clear evidence of increasing violence when the abduction occurs outside of the healthcare setting. In September 2006, a woman came to a St. Clair, MO, mother's home asking to use the phone, slashed the mother's throat, and left with her newborn infant. In court papers, authorities said the suspect was drawn to the home of the newborn's mother by a lawn sign that said "It's a girl."<sup>4</sup> Unfortunately, the issue of home abductions is not limited to infants who have been birthed. In December 2004, a woman who was desperate for another child to shore up her marriage came into the house of a Skidmore, MO, woman on the pretext of buying a dog, overpowered, and strangled the mother of an unborn child. She then cut into her abdomen and removed her unborn baby.<sup>5</sup> In July 2008, a Kennewick, WA, mother was fatally stabbed multiple times and her baby cut from her womb.<sup>6</sup> The NCMEC has tracked 10 fetus abductions or attempted abductions since 1987. In some situations, the initial relationship between mother and the abductor is forged at the HCF. In a 2006 Lubbock, TX, infant abduction, a stranger posing as a nurse visited the new mother several times in the hospital, and then came to mother's home. The women went for a walk together, and when the new mother

---

# baby safety

***The maternity center staff has some important hints for you to keep your new baby safe:***

**1. Never leave your baby alone.**

If you wish to shower or sleep undisturbed, return your baby to the nursery where the infant will be constantly observed by a staff member.

**2. Place your baby's crib in constant view.**

This will allow you to observe any visitors or hospital staff as they approach the baby.

**3. Feel free to question anyone entering your room.**

All staff who are allowed to handle your baby wear their photo ID badges. Your nurse will explain these badges in more detail. If you are uncomfortable with anyone entering your room to take your baby, ask to see the photo ID or use the nurse call light to have your nurse assist in the identification. A staff member working with your baby will know the identification band number that is exclusive to you and your baby.

**Never** give your baby to anyone that cannot show these **two forms of identification**.

**4. Always transport your baby in the crib.**

When going from the nursery to your room, or your room to the nursery, always put the baby in the crib and push the crib. You will find the crib pushes easier and more safely if you guide it end to end, not sideways.

**5. Remember, there are many people who work in the hospital, but only the maternity center staff have special photo ID badges.**

If you have any questions or are unsure about any of these people, please press your nurse call light.

**6. When you leave the hospital, continue safeguarding your baby.**

At home never open the door for people you do not know. Never leave your baby alone in the car, even with the doors locked. Be sure you know how to identify a visiting nurse/helper **before** they arrive, if one is coming to your home.

I understand these safety precautions and I will do all I can to keep my baby safe.




---

 Parent Signature

Nurs 2957 9/95 NS

---

**FIGURE 20-1** Parental security briefing form (Courtesy of Central Iowa Health System).



FIGURE 20-2 Security education poster for parents (Courtesy of Central Iowa Health System).

was distracted for a moment, her baby was gone.<sup>7</sup> If follow-up home care is provided, the identification protocols used by the facility and other security precautions must be thoroughly communicated to the family. Facilities that do not provide home care should specifically communicate that message to help new parents guard against someone falsely representing themselves as being from the healthcare organization and gaining access into the home.

NCMEC attributes the decline of infant abductions from healthcare facilities in recent years to the preventive education program provided to staff and parents. In 1991, there were a total of 17 infant abductions nationwide, 11 of them from healthcare facilities. By December 2008, there were a total of five infant abductions nationwide, with only two abductions from healthcare facilities.

## Physical and Electronic Security Safeguards

The third basic element of infant security involves the installation of certain physical and electronic security safeguards, including strict access control to the nursery and restricted access to the unit, video surveillance of everyone entering the birth center through the main entrance and leaving the birth center regardless of the exit, and where appropriate, the use of infant monitoring.

### *Access Control*

Research has demonstrated that the typical abductor will shop more than one HCF before committing the act of infant abduction. To enhance the real and perceived security of infants, strong consideration should be given to restricting access in and out of the unit. All stairwell and exit doors on the perimeter of the maternity unit should have alarms that will alert unit personnel of their use. Ideally, these doors are equipped with devices that allow authorized staff entry/exit use without activating the alarm and delay the exit of an unauthorized user for 15–30 seconds. All exit-control devices must conform to the AHJ. The most user-friendly and staff-convenient access control measures have devices that allow staff to communicate with visitors and provide the ability to remotely allow entry. The video/intercom door phones discussed in *Chapter 18, Electronic Security System Integration*, are frequently used. Monitored by unit staff and placed at a strategic yet convenient location inside the unit, these devices allow unit staff members to see, talk with, and remotely allow entry into the unit with minimal disruption. Installation should be considered for the main entrance to the unit and other commonly used staff/physician entrances.

All nursery doors should be locked. The door utilized for entry and exit of staff/visitors should be equipped with self-closing hardware. An exception to all locked nursery doors would be when there is an access control person (security officer, receptionist, or unit clerk) stationed at the door for the specific purpose of controlling and authorizing access. Lounges, locker rooms, and/or storage rooms on the unit should also be under strict access control at all times.

### *Video Surveillance*

A key to the successful recovery of an infant is largely based on having a video surveillance system properly installed and designed to obtain a full face shot of all persons leaving the unit. Several operating philosophies to the video surveillance system should be in place and are identified in [Table 20-4](#).

There is no specific mandate that video surveillance systems utilized for infant security need to be live monitored. In most systems, however, there is live monitoring capability of all, or selected, cameras at the main nursing station. In addition, many systems will include redundant monitoring at the facility's central security station along with redundant alarm monitoring.

**Table 20-4** Video Surveillance Operating Philosophies in Infant Care Areas

Infant Security Video Surveillance Strategies
<ul style="list-style-type: none"> <li>• Full surveillance of each exit point from the unit to observe each entrance, exit, nursery entrance, hallway, stairwell, and elevator door on or near the infant care unit(s)</li> <li>• Cameras may be “live” on a continuous basis or activated upon door use</li> <li>• Position color monitors at nursing stations placed in locations so the public does not see the images</li> <li>• All cameras are in color and recorded; a minimum 10-day library must be maintained</li> <li>• Prominent signage stating that all persons are recorded for security purposes (remember the message being sent to a potential abductor if/when they shop your facility)</li> </ul>



As discussed in previous chapters, a testing, repair, and maintenance program must be created to verify that the system is in proper working order and functioning at all times. A structured monthly verification protocol is suggested.

## Electronic Infant Monitoring

There has been a good deal of interest by healthcare security organizations in the electronic monitoring of infants. These systems have been developed and refined over the past few years and now provide a wide range of products. The design of an electronic infant monitoring system begins with defining the space to be protected, often referred to as the *protection zone*, or *safe area*.

The basic electronic infant monitoring system is one that simply sounds an alarm when the device on the infant is detected by a receiving unit at a specific point. Infant monitoring systems used for just this basic purpose are proven to be ineffective. The infant security system should be integrated with door and elevator controls, and video surveillance systems to accentuate the protection of infants and harden the organization as a target for a potential abductor. The proactive use of an infant monitoring system is credited for preventing an abduction at Nashville General Hospital at Meharry in Nashville, TN, after an abductor was able to take a newborn from the mother's room but was prevented from leaving when the system immediately locked down the women's services area within the hospital. Within minutes, the abductor handed the newborn to a doctor as she could not leave the unit.<sup>8</sup> Infant monitoring systems will cost anywhere from several thousand dollars for a single door alarm to several hundred thousand dollars for a very sophisticated system. However, the decision to install any electronic monitoring system should not be based on funding alone. There must be a complete buy-in by unit staff, as these systems require human involvement to make them effective. There is considerable staff task and administrative time required in the daily operations of these systems. The large number of nuisance (false) alarms poses significant risk to the overall posture of infant security at many birthing centers using these systems. Unit staff members and security can become immune to large numbers of alarms and as such, the system

**Table 20-5** Reduction Strategies for Infant Monitoring Systems**Infant Monitoring Alarm Reduction Strategies**

- Creating a multidisciplinary task force charged with addressing this; involve representatives from the mother/baby unit, security, facilities, and the manufacturer's representative.
- Develop a performance measurement and track each alarm; determine if the alarms are staff generated, parent generated, or system failures. Implement strategies based on analysis of the same.
- Closely review the placement and range of the "exciter fields"; incorporate shielding as appropriate.
- Denote the range of each exciter field in a visible and obvious manner (meeting all aesthetic requirements); this can be done with carpet, tile, etc. Incorporate this information into both unit staff and parental education.
- Close all doors to the unit and adjust system functionality to secure doors if a tag enters an exciter field; the system should not alarm unless the door is open. This allows "mom" to walk around the unit without setting off an alarm.

does not operate as designed and be effective. Each organization using electronic infant monitoring should implement strategies to minimize the number of alarms generated. Several strategies are identified in [Table 20-5](#).

No matter what form of attachment bands (or clamps) are in use with the electronic tagging of infants, HCFs should be very careful to ensure that there is never any delay in activation of the alarm function upon separation from the infant and perform frequent testing in support of that guideline. Staff should be trained to respond immediately so there is no delay between detection of the alarm condition and generation of the alarm notification. Staff members should never adopt a philosophy of only turning the system on when they suspect a possible problem. Such actions present major liability risks. Detailed records should be documented on testing procedures and preventative-maintenance schedules. Weekly tests should be established to verify that the infant tagging system is operationally functional and in good working order using a randomly selected tag (not a test tag) with each area (portal of exit) covered by the system. A more detailed review of electronic infant monitoring systems is found in *Chapter 18, Electronic Security System Integration*.

## General Security Precautions and Guidelines

The NCMEC document previously referred to covers a number of fundamental elements of infant security. It should thus be reviewed by all persons having responsibility for protecting infants. The following is a general summary of some very important aspects of infant protection while in the hospital, at discharge, and at home:

- Infants should be transported one at a time and never left alone in a corridor.
- Infants should be transported in a bassinet, never arm-carried, except in an extreme emergency.
- There should be no posting of personal information of the mother or infant to the public when in the facility.

- Infants should always be in direct line-of-sight supervision by staff or mother/family.
- Infant bassinets in the mother's room should be placed on the side of the bed farthest from the room entry door.
- Birth announcements should not be published in the newspapers or online media; if birth announcements are used, announcements should use surnames and refrain from including the family's home address or telephone number.
- Staff should provide internal transportation to the discharge point and remain with the mother/infant until their departure.
- Parents, family, and friends should avoid using outdoor decorations announcing the infant's arrival at home.

Only well-known and properly identified persons should be allowed into the home. Authorized caregivers should provide advance information of the intended visit and produce proper identification that has been previously explained to the infant's mother/family. The HCF should develop a written plan defining all proactive measures to take to prevent infant abductions in the labor and delivery unit, postpartum, overflow and VIP units, and pediatric care locations.

### Critical Incident Response Plan

The response to an infant abduction should be considered a whole-house plan, as all organizational staff should be actively involved. There should be a code name for this response that is communicated to as many staff as possible, usually via an overhead paging system and group alert communication device, if available. A common code, and recommended by the NCMEC and IAHS, to be utilized by HCFs to activate the infant abduction plan is Code Pink. In the event of an abduction, the immediate involvement of law enforcement and the media is paramount in terms of enhancing a successful outcome. Most often, infants are recovered as a direct result of information generated by media coverage.

The infant abduction response plan should appropriately define the role and responsibilities of nursing, security, public relations, law enforcement, and the facility-wide responses. This includes the need to immediately search the unit, notify security, and protect the potential crime scene.

#### *Unit Nursing Personnel*

Unit staff must be calm and sincere in their involvement and immediately search the entire unit. Immediately and simultaneously, the nursing staff should contact security. At no time should a practice be instituted to require verification of a missing infant prior to calling. This creates undue delay if there is an actual event. An important role is for the assigned care provider to stay with the mother during the event. Organizations who have experienced abductions have found moving the mother to a more isolated area within the facility beneficial to her health while removing her from the crime scene that must be immediately protected.

### *Facility-Wide Staff*

A common challenge for many healthcare organizations is not being able to clearly hear overhead codes. Overhead announcements should be clearly announced initially three times and every 5 minutes until an “all clear” is generated. The process should reflect the responsibility of notifying parking attendants, valets, and other external workers on campus. When Code Pink is announced overhead, facility-wide staff members must know their role and what to look for. All staff members must know to look for suspicious behavior, such as possibly carrying a travel bag that could contain an infant, rushing with an infant, and/or transporting a baby/infant without a bassinet.

A common discrepancy found with employee response to an infant abduction is what to do if someone is seen who looks suspicious and meets the criteria above. Responding employees should have the responsibility to stop suspicious individuals and question them to see what is in their bag, backpack, etc. Research has found that employees do not know what to do in the event the suspicious person does not comply with the request. If such situation were to occur, the employee should remember that the safety of the infant is the first priority. Nothing should be done to cause a potential abductor to harm the infant. Education and training of employees should focus on staying calm and to:

- Approach in a nonthreatening manner, facing the person at a safe distance.
- Speak with a calm, steady voice, explaining that the facility is on alert for a possible infant abduction and that everyone is being stopped.
- Instruct the nearest bystander or employee to call for security assistance immediately.
- Attempt to delay the suspect by keeping him/her in front of you (walk backward slowly if necessary).

If an employee is unsuccessful in preventing the suspect from leaving, he/she should be instructed to never physically touch them or do anything that could possibly endanger the infant while making note of the following:

- Identifying features of the person
- Bags or bundles carried
- Route of exit
- Vehicle description and license plate number

A timely response is every employee’s responsibility. Following these simple steps can improve the healthcare organization’s chances of a successful recovery of the infant.

### *Security Staff Response*

The March 2008 abduction at Central Florida Regional Hospital in Orlando was a significant event for the parents, the hospital, and the community as a whole. The incident was also an important lesson for how security staff should be deployed during a critical incident response to an infant abduction. The security staff responded to the main entrance of the campus and saw a heavysset woman carrying a package as she entered



her vehicle. The officer was unsuccessful in stopping the vehicle but was able to obtain a vehicle description and partial license plate number. As a result of that information, law enforcement officers were able to quickly locate the abductor and successfully recover the infant.<sup>9</sup> The significance of this experience is the universal change in response security personnel have undertaken. Today, it is expected that the security staff will immediately respond to perimeter points of the grounds or campus of the facility. Only after securing the perimeter should a search of the interior/exterior of the facility be initiated by security, and then control of the crime scene transferred from the nursing staff. Historical practices placed more emphasis on responding to facility access points, crime scene preservation, and not responding to the campus perimeter. This philosophical change requires every healthcare security program to have a policy that defines who and how to safely stop and search a vehicle during an event. The policy should also include actions to be followed when the driver of the vehicle fails to stop or allow staff to search their vehicle.

Security staff should secure the current day and previous 10-days' video recordings when an event occurs—at the facility or in the community. Additionally, the security department should be prepared to provide technical support and confidential viewing if the police department cannot access the recordings on their equipment. Law enforcement liaison and planning is essential as most agencies have limited familiarity with the issue of infant abduction from HCFs. Providing a general awareness of the facility will assist the agency in planning their response. Many healthcare organizations invite law enforcement to be involved in the creation and review process of the critical incident response plan and participate in the exercising of the infant abduction response plan.

It is extremely important for both the healthcare organization and law enforcement authority to contact the NCMEC for technical assistance in handling an infant or pediatric abduction. The NCMEC's 24-hour telephone number is 1-800-843-5678.

### *Communications, Media Relations, and Involvement*

Every healthcare organization should be prepared for using the media to aid in its recovery efforts of an abducted infant. Most often, infants are recovered as a direct result of the leads generated by media coverage of the abduction, which includes the release of appropriate video images. The organizational media plan in response to an infant abduction should be designed to:

- Identify an official facility spokesperson
- Mandate that all information is cleared by facility and law enforcement authorities before it is released
- Keep from panicking the abductor into abandoning or harming the infant
- Solicit the assistance of other HCFs in the community/region

Healthcare organizations are encouraged to develop a specific form to report suspicious behavior with nearby facilities and other nursing units inside the facility. If an event does occur in the community or region, every HCF should review captured images from

their video surveillance system to verify if the abductor shopped their HCFs. Captured images can help prosecutors build their case against the alleged perpetrator while validating the effectiveness of the organization's infant security plan.

### *Drills and Exercises*

TJC standards and elements of performance do not require infant/child abduction drills. The standards do require that the organization identifies and implements security procedures that address handling of an infant or pediatric abduction, as applicable. An infant abduction exercise is one method to evaluate the effectiveness of the procedures regarding this issue. It is up to the organization to determine the appropriate actions to ensure successful implementation of security procedures.<sup>10</sup>

Infant/pediatric abduction drills should be conducted on a schedule that includes personnel who work days, evenings, weekends, and/or nontraditional shifts in addition to testing the response of the pediatric care areas. Drills should never be viewed as a “success” or “failure” for the sole reason that the mock abductor is able to successfully carry out the exercise without being stopped. The goal for each exercise should be to teach and test using a mixture of announced and unannounced exercises. Never should an inpatient mother unknowingly be involved in a drill. As a result, an important safeguard in the infant security plan is not tested and the simulation modified. However, engaging a real mother in activating the Code (but not using her infant) is a useful tool to engage staff participation. Obtaining the mother's knowledge of her role in her infant's security in the critique provides a snapshot of the effectiveness of the parental education provided.

Evaluations should include a critique of the responses of unit staff, security, PBX announcement, and the facility-wide response to include the time taken to initiate the response. Monitoring the time it takes from the initial call for a Code Pink and the time it takes for the hospital operator to announce overhead is an important performance indicator. A sample infant abduction evaluation form/report card is demonstrated in [Figure 20-3](#).

Prior to conducting the exercise, the infant abduction drill should have the mock abductor visit and call the unit prior to the actual drill. This pre-scout methodology is a useful tool as it allows the mock abductor to obtain information on department layout and the security measures in place, plan the escape route on the basis of the information obtained, determine how much information on a patient can be gathered, and evaluate staff response to an individual asking questions and demonstrating traits of the typical abductor.

## **Infant Discharged to the Wrong Family**

The discharge of an infant to the wrong family is a significant event, but not actually a breach of security. The security department may become involved with such a situation as a resource to investigate the occurrence and contribute to a successful outcome. However, the proper discharge of a patient is a clinical management function.

As a matter of protocol, every birthing center should give strong consideration to having the mother participate in the band-verification process every time her infant is

**Sample  
Infant Abduction Drill Evaluation & Scorecard**

Drill Information:

Campus: \_\_\_\_\_

Date: \_\_\_\_\_

Building: \_\_\_\_\_

Floor: \_\_\_\_\_

Victim  
Age: \_\_\_\_\_ Gender: \_\_\_\_\_ Male / Female

Ethnicity: \_\_\_\_\_

Scale: Circle one
1-Poor
2-Fair
3-Good
4 -Very Good
5-Excellent

1. The announcement of the Code Pink was provided correctly over the Public Address System and was heard in all areas of the campus (Number and Letter after "Code Pink + Location" to identify age and gender M/F of missing person).  

1 2 3 4 5
2. Upon notification of abduction via the overhead announcement, staff responded with a sense of urgency and seriousness.  

1 2 3 4 5
3. Upon notification of abduction, staff quickly proceeded to egress points to secure the exits and stairwells in their area.  

1 2 3 4 5
4. Upon notification of abduction, staff initiated a logical and focused search of their area as specified in their policy and procedure.  

1 2 3 4 5
5. Hospital associates challenged all visitors/suspicious persons observed with infants meeting the Code Pink announcement criteria and/or carrying bags or containers large enough to conceal an infant or small child.
6. Was anyone suspicious stopped?  
 Yes /No  
 If so, please describe how the person stopping them handled the situation. (i.e., what was said to them, was security contacted, did security respond, etc.).  

1 2 3 4 5
7. The Charge Person or designee in every department initiated the proper search Plan and took charge of their area.  

1 2 3 4 5
8. The video surveillance system was able to be utilized for reviewing camera surveillance of facility for post-investigative purposes by the security department and law enforcement personnel.  

1 2 3 4 5
9. The emergency response provided by the Emergency Response Team (ERT) was timely and appropriate.  

1 2 3 4 5

Additional  
Comments: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

FIGURE 20-3 Sample infant abduction drill evaluation form.

returned to her room. This process further ensures that staff members are matching the correct mother and baby, helping to prevent mistakes and the negative feelings (and press) associated with the event.

## Special Care Nursery, Pediatric Care, and Overflow Areas

As targets within the birth center have hardened, abductors have had to look elsewhere in the HCF. As a result, abduction from pediatric care areas is now the second most common area where abductions occur. Most HCFs have several inconsistencies with the protection measures in place within their birthing center as compared to other locations within the HCF that cares for infants. It is recommended that similar and consistent security protocols be implemented in special care nurseries, pediatric care, and postpartum overflow areas. In some situations, the consistent application of all protection safeguards used in the birth center may not be feasible or appropriate; i.e., an infant tagging system may not realistically be needed in the special care nursery. In such instances, the healthcare security administrator and unit manager should document what protection measures are taken in lieu of those not used or consistent with the birthing center. Often, nontraditional security safeguards are identified, which include one-to-one patient-to-staff ratios or constant parental presence. If an overflow area must be utilized outside of the protected department, a common safeguard is to locate the patient in close proximity to the nursing station, enhance security visibility in the area, and provide additional parental education on the importance of their involvement in their child's security. What should not fluctuate, however, is the critical incident abduction response plan. Much debate surrounds the use of the same code for infant and pediatric patients. It is a commonly held belief by healthcare security professionals and the NCMEC that the same code should not be used for each. Many HCFs differentiate between the abduction of an infant and the pediatric patient by adding the age of the child at the end of the code: i.e., "Code Pink-3." The code words currently used by law enforcement and retailers such as CODE AMBER and CODE ADAM should be strictly avoided to represent infant abductions or missing children in the healthcare setting.

### *Family Abductions*

While nonfamily infant abductions are thought to be the greatest risk, a more common concern is the abduction of an infant or child by a family member. Whether a custody dispute, child abuse, or social services intervention, this problem is widespread in the healthcare environment. Because these cases involve abuse and/or neglect issues, the NCMEC has deemed these children to be at greater risk than newborn infants taken by nonfamily members. The NCMEC has identified several factors noted in [Table 20-6](#) that should be taken into consideration when establishing protection strategies for this vulnerable patient population.

## ED Security

A gunman entered a San Diego hospital emergency room and started shooting indiscriminately, killing two and wounding two. A social worker was killed in a hospital emergency

**Table 20-6** Protection Strategies for the Risk of Family Child Abduction**Family Abduction Protection Strategies**

- “Red flagging” the child’s name in the system to indicate no information is to be released
- Admitting the child under an assumed name
- Placing the child in an isolation room or in the intensive care unit
- Placing an assumed name on the child’s door
- Using wireless video surveillance with a monitor at the nurses’ station to closely watch the child
- Increasing frequency of observation in the patient’s area
- Posting a description of the potential abductor with security, nursing, and the front desk or reception area
- Posting a security officer at the patient’s room/floor/unit

*Courtesy National Center for Missing and Exploited Children, Alexandria, Virginia.*

room in Pittsburgh by an assailant who also took three people hostage. A man dressed in a security uniform walked into an Atlanta hospital emergency room, where he shot four people and then committed suicide. A man entered a metro Denver trauma center, pulled a gun on the security officer controlling access to the treatment area, forced entry, and killed himself in front of the ED nurses’ station. These types of incidents are frequent occurrences in EDs in the United States and throughout the world. The ED will always have the characteristics that warn of disruptive behavior. Extreme mental and physical factors, acute psychiatric manifestations, drug and alcohol abuse by patients and visitors, the mix of patients and service providers outside the medical staff (i.e., police, fire, ambulance, coroner, and so on), and often chaotic circumstances combine to produce a unique environment. When coupled with rival gang members who show up with guns because a prominent gang member is brought into the hospital, lengthy wait times due to continued overcrowding, and the everyday threats of caring for victims of domestic violence, EDs are without question the most volatile area in the healthcare setting. In fact, the emergency room chief at San Francisco General reports that threats from angry patients and/or visitors occur daily, and violence breaks out at least once a week. Dr. David Golan, an emergency room physician at the University Medical Center in Las Vegas, NV, sums up the security concerns in emergency rooms when he says:

“What is happening in emergency rooms is just insane. We give people who say they are going to kill people a chance to do it. No restraints, no metal detectors. The truth is; I think emergency room policies are crazier than some of the people we see.”<sup>11</sup>

Dr. Golan was part of a real-life drama played out in March 2008 when a patient shattered his nose after the patient had previously told the doctor that he was going to kill him. What Dr. Golan is talking about are the constraints being placed by regulatory and accreditation agencies to apply medical restraints (physical or chemical) before certain things must happen. Today, interpretations of CMS guidelines have created a wait-and-watch attitude versus a proactive approach to using restraint as tools to address the escalating violence occurring in EDs. Unfortunately, these interpretations have contributed to the ever-increasing volume of assaults against, and subsequent injuries to, care providers, security officers, and others who work in the ED.

In a 2007 survey conducted by the Emergency Nurses Association, 9 out of 10 Emergency Department Managers cited patient violence as the greatest threat to department personnel.<sup>12</sup> As discussed in great detail in *Chapter 19, Preventing and Managing Healthcare Conflict and Violence*, the physicians and nurses who staff EDs are demanding greater protection by hospitals. Disruptive behavior is predictable, and it can be managed to minimize the risk in providing safety for all concerned. The IAHS has developed a basic security industry guideline for HCFs that provide emergency care services.

#### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #09.03

##### **Security in the Emergency Care Setting**

**STATEMENT:** Healthcare facilities (HCFs) that provide emergency care have special security needs and should have a security plan specific for that department.

##### **INTENT:**

- a. The plan should be based on identified risks for the ED including volume, types of patients treated, and incident activity.
- b. The security administrator should be involved in the planning and building phases of ED construction and renovation as a resource relative to security design issues.
  1. The ED waiting area should be separated from the ED treatment area and be self-contained to include independent access to restrooms, telephones, and vending machines.
  2. Access controls should be in place to control and limit access of ED visitors into the ED treatment area and into the main hospital.
  3. A room or area within the ED, separate from other patients, should be available for the treatment of behavioral health patients. Consideration for this room should include visibility by staff and the removal of items that could be used by the patient to injure himself/herself or others.
  4. The ambulance entrance should be separate from the walk-in emergency entrance and waiting room.
- c. Security staff provides support services in the care and control of the ED. These services are to be provided at the request and under the direction and supervision of clinical staff unless circumstances require immediate action to prevent injury or destruction of property. (See IAHS Guideline 02.04, Security Role in Patient Management.)
- d. Security equipment and systems to protect staff and patients should be in place. These may include electronic access control, cameras, and panic alarms. The ED should be capable of being locked down in the event of an emergency.
- e. Physical measures and/or procedures should be in place to deter the elopement or removal of patients at risk of harming themselves, others, or of being harmed.
- f. ED staff (including security staff) should receive ongoing training in workplace violence, crisis prevention intervention/violent patient management to recognize, avoid, diffuse, and respond to potentially violent situations.

- g. Periodic meetings, at a minimum annually, with multidisciplinary staff should be conducted to review security protocols and resolve security issues within the ED.
- h. Policies and procedures should be established for security's role in managing patient watches, holds, and restraints.

**REFERENCES/GENERAL INFORMATION:**

- Emergency Nurses Association, Position Statement, Violence in the Emergency Care Setting, Developed 1991, revised and approved by the ENA Board of Directors, September 2008, ENA Web Site: <http://www.ena.org/about/position/PDFs/64CAB0B9EFD44C4A51CCBF0F30D7DD3.PDF>
- IAHS5 Guideline 02.04, Security Role in Patient Management

**Approved:** December 2006

**Last Revised:** October 2008

## How Much ED Security Is Needed?

Every hospital that has an ED must assess its own specific vulnerabilities and apply the degree of security necessary to maintain a reasonably safe and secure department. It is important to remember that the ED is made up of several distinct areas, and all bring their own unique security considerations. Among the chief assessment considerations are:

- Annual volume of emergency care patient admissions
- Trauma level designation
- Primary service area and types of patients and visitors typically seen
- Specialized services offered such as psychiatric or forensic patient agreements
- History with aggressive patients in treatment areas
- Expectations of security staff for patient assistance
- Average amount of time spent by security staff on patient assistance
- Area's crime rate (or propensity for crime)
- Layout and design of the ED

A variety of safeguards can be applied to any ED, but it is the degree of application of a specific safeguard to establish proper security that must be determined. For example, one ED may require only periodic security patrols, another may require the presence of an officer at night, and another may require 24-hour security coverage by one or more officers. Security practices should be consistent with event-driven policies and procedures. It is difficult to convince management and staff to maintain the highest levels of security when all is well in their work environment. If the security plan adjusts with situational circumstances, the ED staff is more likely to be active participants.

As in all situations involving patient care, security officers must act in the best interest of the patient and follow the instructions of the care provider to ensure no disruption in the flow of healthcare. Walt Sarratt, Director of Security and Safety at Hillcrest Baptist

Medical Center in Waco, TX, shares that the success of security is “dependent upon the ability to deliver our message in a manner that does not infringe upon a caregiver’s prerogative to prioritize patient care in a manner that is best for all concerned. The opportunities for misinterpretation are endless in an environment where emergencies are commonplace, and the nature of prioritizing treatment is complex.”<sup>13</sup>

## Security Design Considerations for EDs

The design of the ED begins with the security risk assessment. The assessment should include the security administrator and ED leadership reviewing key areas such as:

- Driveway and parking area layout
- Entrance points to the waiting and medical treatment areas
- Compartmentalization of the waiting area and medical treatment area
- Protection for triage and front-desk personnel
- Patient/visitor flow through the department (from the parking lot to the waiting room to the patient care area through discharge); room design and location to include line-of-sight visibility and exit pathways
- Creation of a sterile environment for at-risk patients
- Use and deployment of physical and electronic security safeguards

An armed fortress is not what should be created. The healthcare security administrator should create an environment using the principles of Crime Prevention through Environmental Design (CPTED) to guide how the physical design of the ED can work for better personal safety and patient-focused care.

### *Driveway/Parking Area Security*

Dedicated parking is provided by most HCFs for their emergency care patients. The area, typically located in close proximity to the ambulatory entrance of the ED, should be well lit and monitored for appropriate use. Way-finding signage should easily guide patients and visitors to the dedicated parking area from each entrance to the healthcare campus. Solid physical barriers and curb markings should separate the driveway from sidewalks and facility entrances. Whenever possible, there should be distinction between the ambulance entrance and patient parking that is clearly marked and provides a reasonable degree of separation between the two. Disrupting the line of sight between the patient drop-off and ambulance bay off-loading is recommended using either physical or visual barriers. In many cold weather climates, a number of healthcare organizations have incorporated enclosed ambulance bay garages that further separate these two areas. General design considerations and protection measures used for healthcare parking areas are covered in greater detail in *Chapter 23, Parking Control, and Security*.

### *Walk-in Area/Waiting and Admissions*

Many security incidents involve visitors and occur in the walk-in area. Visitors may include family members, friends, or even enemies of the patient. The waiting area should contain washrooms, vending equipment, and telephones. Long waits and tense visitors



can create trouble, if not properly managed. There should be distractions to help the time pass. Televisions, Internet access, and magazines are helpful. Proper placement helps to further compartmentalize the waiting area. An important part of this management is to keep visitors informed; the lack of information often stimulates incidents. Just speaking with a patient or visitor can help alleviate tension. Emergency medical care units must be staffed and organized to effectively communicate with those persons waiting for a sick or injured patient being treated or in need of treatment. The conversation should be simple but often enough to help patients and visitors to not feel ignored. Providing the chance to verbalize frustrations is a proven and effective de-escalation technique.

Many healthcare organizations strategically locate video surveillance cameras in the ED waiting area to monitor activity and deter unwanted behavior. An emerging trend in very active EDs is the placement of video monitors in the waiting area displaying camera images. A basic crime-prevention technique, the practice is believed to enhance the psychological deterrence of the cameras as patients and visitors are more fully aware of the video surveillance system.

### *Triage and Front-Desk Reception*

In most cases, the first person the patients and visitors encounter is a receptionist or triage nurse. It is imperative that this point be staffed at all times to greet those who enter. The triage area should be separated from the walk-in area, which is necessary for security and patient confidentiality. Many employee complaints stem from the higher level of security provided to the ED medical treatment area without a similar level of protection for triage, registration, and other front-desk staff often located within the waiting area. Impact-resistant glass has been installed at many healthcare organizations to enhance the protection of these staff. However, a common concern by hospital administrators is the unspoken message generated with the additional measure, specifically its lack of customer-friendly appeal, and the potential hindrance to patient flow. It is recommended that the receptionist or nurse sit inside an enclosed area with a service window. The enclosure should make it difficult for someone to grab the receptionist or to jump over the counter. Some organizations have installed high counters, similar to those used in the banking industry, to create a psychological deterrence against patient and visitor violence. Other organizations have incorporated decorative glass or see-through laminate above the counter to further enhance height while maintaining a more pleasing aesthetic décor in the area. The degree of enclosure depends on the assessed vulnerability. There must of course be a window for communications with the arriving patient to begin the triage process. In the locked triage area, the triage nurse would simply admit the patient to the assessment area, locking the door after entry. It is recommended that all triage areas, locked or unlocked, have two entry/exits, one directly into the treatment area. This prevents a patient from blocking an exit pathway. Upon completion of the triage process, the triage nurse would simply send the patient back to the waiting area to await treatment or take them directly into the treatment area.

Strategically placed duress alarms are useful tools for emergency care staff members working at the front desk, in admissions, and in triage.

### *Compartmentalization of the Medical Treatment Area*

The security layout and design of an ED can be viewed as compartments and control points. A major consideration in providing for safety in the ED is to control the access of patients, visitors, and staff. Historically, these controls varied to some degree for many smaller facilities, according to the day and time; i.e., tighter restrictions imposed during the night hours. Today, however, it is an industry standard practice to restrict access to the ED medical treatment area 24 hours per day, regardless of the size or location of the HCF. A common mistake in this regard is to lock off the treatment area from the waiting room and then leave staff entry–exit doors open, which provides access to other hospital areas and departments. All entry/exit points to the treatment area must be controlled and restrict access to authorized personnel only.

The ambulatory and the ambulance entrances are usually separate. In small departments, these two entrances are often combined during off-peak periods. The ambulance entrance should open directly to a nursing station. The ambulance entrance should be restricted to ambulance drivers and staff using electronic bypass measures such as a card key, a push button lock, or other means to gain access. An electric lock release and audio communications at the nursing station can be used to accommodate entry for others. A clearly marked communications station on the exterior side of the entrance is required, and either direct visual observation or a video surveillance system is required to properly manage the control system. The ambulatory entry point is usually not locked, but it could be, depending on the vulnerability. It is recommended that this entry point be equipped with a lock even if the entry is always open. The purpose of this lock is to have the means to lock down in the case of an unanticipated emergency situation or condition. [Figure 20-4](#) shows a model layout for access control in a small ED.

The access control system for the medical treatment area should be designed to minimize staff inconvenience and identify common working relationships with other departments. Design considerations should look at department staffing after normal business hours, the number of staff members on duty, and a review of traffic flow patterns. Relationships with other frequented departments should also be considered when designing the secured compartment. For instance, if the radiology department is found outside the secured compartment, staff often alter and undermine department protection efforts by propping open secured doors to transport emergency care patients back and forth. Incorporating the radiology department into the secured compartment has become a common practice for many EDs to prevent the automatic door system type of security breach.

### *Quiet/Observation Room*

The quiet or observation room is a room within the treatment area used to administer care to the combative or at-risk patient. In smaller facilities, it may simply be a treatment room that is very sparsely equipped or completely stripped of objects. In large, higher volume facilities, there may be multiple rooms used for this purpose. These rooms may actually be locked and padded with tamperproof hardware items. This type of room

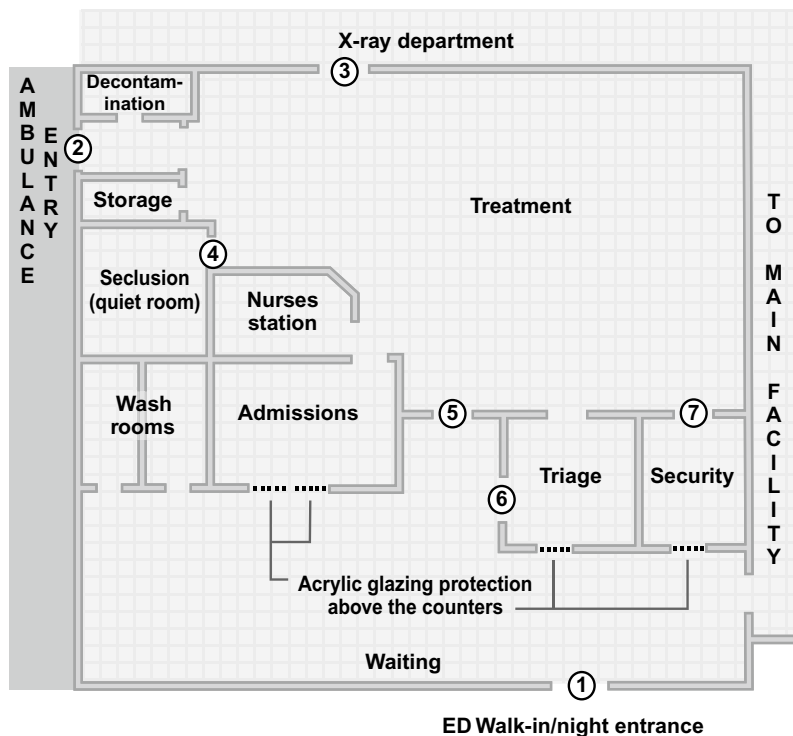


FIGURE 20-4 A model layout for access control in a small ED.

generally has an observation window and/or a video surveillance system. See *Chapter 18, Electronic Security System Integration*, for more detailed information about the use of video surveillance in patient care areas.

#### *Family Consult Room*

The family consult room is a room, preferably located between the waiting and the medical care areas, used for family and friends of a patient who may be very ill or is deceased. It is a place out of the common waiting area, not in the medical care area where family and friends can share emotions or grieve. Ideally, there is open access from the waiting area and restricted access to the medical care area. Family and friends should be escorted from the family consult room into the medical care area.

#### *Safe Room*

The concept of a safe room, primarily in EDs, has emerged as another safeguard in managing workplace violence. A safe room merely means a designated room that can be locked from the inside, as a place for staff, patients, and even visitors to hide in the event of an immediate threat of danger. The typical safe room is a room usually utilized for day-to-day activity and equipped with telephone and/or radio communications equipment. It should

be easily accessible and somewhat centrally located within the department. It is most often a regular treatment room, which may be a distinct advantage if patients are present when the safe room is actually being utilized as such. There are many different scenarios in which the safe room would provide a secure place, such as when trouble erupts or is anticipated. An example of anticipated trouble might be when visitors, or adversarial persons, in a waiting area insist upon going back to the treatment area to see the patient who is being treated. The fear of an altercation or the medical procedure itself may preclude staff allowing such a visit. In this case, it may be a prudent security strategy to provide the patient treatment in the safe room, which could be secured if necessary. Another scenario would include the safety of a specific staff member relative to a domestic situation.

#### *Physical and Electronic Security Safeguards*

A variety of physical and electronic security safeguards can be used when securing the ED. These safeguards include electronic access control equipment, bullet-resistant glazing, duress (panic) alarms, video surveillance, video intercoms, signage, secure storage containers including gun lockers, and metal screening. The application of these safeguards is discussed in detail in *Chapter 17, Physical Security Safeguards*, and *Chapter 18, Electronic Security System Integration*.

### Security Staffing in EDs

There is a need to provide security staff for emergency service departments in a great many HCFs. In small facilities, a patrol and response capability may suffice, but very large EDs may require several fixed security posts on a 24-hour basis. It is quite common to staff emergency rooms with a security officer only at night. This practice can be cost-effective, especially when the officer also controls nighttime visitors for the entire facility. The emergency room is also a logical location for a security operations control center, which provides a certain presence in itself.

The single greatest attributing factor to security staffing in the ED is the expectation of security with patient assistance. As discussed in *Chapter 12, Patient Care Involvement*, responding to requests for assistance with patients is a valid and necessary function of any protection system; however, the scope and expectations of this assistance can significantly drive the amount of security resources dedicated to the ED. Security personnel assigned to emergency treatment areas should be uniformed to achieve maximum effectiveness. Individual hospitals must decide whether to arm officers, weighing all the pros and cons regarding this important decision. With the ever-increasing mental health patient population seeking services in the ED, healthcare administrators and protection professionals alike are encouraged to take their cue from the behavioral health setting and not introduce firearms in the medical treatment area.

As has been discussed in previous chapters, it is generally not desirable to employ off-duty law enforcement personnel as security officers in emergency rooms. The training required is very different; police training is of little value for the function of the emergency

room security officer. Police work as a whole is often measured in terms of arrests, and the security effort is measured in terms of conflict resolution and prevention. This is not to say that police service should not be called when police response is required for a specific incident. Some very busy trauma centers in higher-crime locations have deployed police officers in their ED waiting area with good success. The difference is that the police officer is expected to provide a visible and deterrent value but is not expected to participate in patient care activities. Unfortunately, the costs of the police officer assignment are often more than double that of a security officer.

In numerous hospital security programs, security officers are promoted to the ED, where they have their own specific job description and generally receive higher pay. Funding for the ED security coverage is sometimes provided by the ED. These officers should be considered and treated as much a part of the ED staff as they are members of the security staff.

### *Security Officer Training*

Security personnel stationed in emergency rooms need extensive training. Their training must include recognizing the early symptoms of disruptive behavior, verbal and nonverbal intervention skills, working knowledge of the process of trauma care, the psychology of stress, the role of supporting medical care (not giving advice or administering care), the application of physical restraints as part of a restraint team, and proper take-down procedures. Although these subjects are appropriate for all security personnel, the full-time officers assigned to busy emergency rooms must develop and hone these skills to a greater extent than a generalist.

Training should not be limited to the security staff on an individual basis. There should be joint training exercises of the ED staff and the security staff. This collaborative training is important to establish working protocols and to develop the team concept. Role-playing is a common method used in this training.

### *Interaction Protocols*

Whenever security personnel support the ED, formally established protocols, or guidelines, must govern the actions of the officers and the ED staff. Without these guidelines, there is bound to be conflict and dissension between security and ED personnel on how specific situations are to be handled. The objective is to eliminate individual expectations and guesswork. Firmly established rules for different situations eliminate dissatisfaction and provide a high level of service. Generally, nurses or physicians take charge in dealing with patient incidents, and security officers take charge in dealing with visitor problems outside the treatment area. Visitors within the treatment area occupy a middle ground, but generally are in the purview of the medical caregiver. The issue of managing at-risk patient behavior and the corresponding roles of security and care providers is discussed in detail in *Chapter 12, Patient Care Involvement*. The term *patient assistance* is sometimes used to describe the activity of standing by to watch a particular patient. Officers are generally asked to perform a patient watch when a patient causes staff to feel fear,

anger, uneasiness, potential danger, or when there is an indication that the patient may attempt to leave prior to proper medical evaluation or treatment. Staff members must recognize the considerable range of these feelings and assess the gravity of the risk they perceive. Although this discussion focuses on patients, the same evaluations, preparations, and actions are required for visitors in treatment areas, waiting areas, or patient rooms outside the ED.

### *Policies and Procedures*

It is important to take the ambiguity out of how security practices work in the ED. Policies and procedures provide staff guidance and help keep practices consistent regardless of the situation. Consider policies for each of the following:

- At-risk admissions
- Patient searches
- Event-driven security plan
- Metal detection
- Elopement/escape precautions
- Access control
- Visitation control

### *Visitor Control*

An emerging safeguard is the incorporation of visitor control policies and procedures to restrict the number of visitors who can accompany a patient in the medical treatment area. St. Anthony's Central Hospital, a Level I trauma center in Denver, CO, uses a simple color-coded visitor pass system. Each patient is limited to two visitors at any given time. The passes, issued by a security officer, change color daily and are shared between family members. Access to the treatment area is granted only by visitors who are in possession of the pass. A similar visitor pass system is in use at Yuma Regional Medical Center, a regional trauma center in Yuma, AZ. Security personnel maintain a two-pass system for each ED patient room and grant access only to visitors who have been issued the pass. A daily inventory is conducted to verify all passes are returned or new room-specific passes are generated. Care providers typically like having visitor control procedures in place as it limits the large number of interruptions they incur from too many visitors.

## **ED Staff Education**

Confidence to work in the ED starts with knowing there is an organizational plan to address the security risks within the security department. More than just teaching staff to recognize and respond to escalating tension with emergency care patients, care providers must learn to take ownership of their work environment. The acronym POWER shown in [Table 20-7](#) helps ED personnel recognize, understand, react, and manage their environment.

**Table 20-7** Power Principle to Emergency Department Security Education

Emergency Department Security Training	
<b>P</b>	<b>Prepare for your patient.</b> Use all your resources to determine the emotional state of the patient. This may include the patient's previous care history, information from the transporting EMS/police, or precautionary notes from your co-workers. Remember to always give yourself permission to think personal safety first.
<b>O</b>	<b>Own your work environment.</b> Begin with everyday proactive safety plans that lead to a safer work environment. Know how the room and the equipment in the room work for or against creating a safe work environment. Have the confidence to proactively take charge of your place of work.
<b>W</b>	<b>Work within your training.</b> Be an active participant in the organization's security plan. Know your training, what you are good at, and what you need help with. Understand the power of having a plan and working together as a team.
<b>E</b>	<b>Expect the unexpected.</b> Complacency can lead to mistakes and unfortunate surprises, especially when dealing with at-risk patients. Mentally working through your options may provide you with the crucial opening necessary to avoid a difficult situation.
<b>R</b>	<b>Remember your resources.</b> There always seem to be more resources for those who are prepared. One employee looks at the metal surgical tray in the patient room as a place to set instruments, while another sees it as a shield to use against an edged weapon. Resources are everywhere if you open your eyes to the possibilities: training, fellow staff members, family, room setup, having a plan, and most of all being an active participant in your own personal safety plan.

*Courtesy of Alan Butler and HSS Inc.*

ED training should be accomplished using a multidisciplinary approach. Training as a team provides the opportunity for care providers and security officers to learn together. Having an understanding of each other's perspective helps build teamwork and a better appreciation for the role each plays in managing the emergency care environment. Role conflict can be a problem for many care providers who struggle between being a patient-focused provider and protecting their own personal safety. It is important for health-care providers to know that both have a place. Take, for example, the care provider who is informed of a difficult patient and then ignores the advice and walks into the patient room. Patient-focused care is not provided when multiple coworkers have to be called to restrain the agitated and physically acting-out patient. There must be acknowledgment that a patient may be difficult. Once this is identified, good personal safety precautions can be taken, conflict avoided, and patient-focused care provided. Personal safety of the care provider must be given first consideration. Staff must be given specific training on how to recognize when escalating situations exist and what to do when this escalation occurs. The risk of disruptive or harmful behavior is easily escalated if inappropriate steps are taken. The overall goal is to maintain safety for everyone involved, including the patient.

Aggression management and response training are important cornerstones to any ED security training. Care providers, security officers, and anyone responding to escalating situations must be able to recognize, understand, react to, and manage environmental changes through the various stages of escalation. This training is discussed in further detail in *Chapter 9, Training and Development*, and *Chapter 19, Preventing and Managing Healthcare Conflict and Violence*.

## Emergency Signals

The ED should have a system of alerting other staff members of an emergency or escalating situation that requires immediate help. These systems are used primarily to summon additional medical assistance, but they may also serve as an element of the security system. Wall buttons, pull chains, and foot or other activation devices should be strategically located within the department, with particular attention given to isolated areas. The device must be placed so that staff members can easily access it, but it does not invite improper activation by patients, visitors, or even staff. There are also available devices that the caregiver can carry (as a pendant or clip-on device) to summon assistance. These devices are more costly than fixed-location devices as the equipment must be able to track the movement of the person to fix the location when the device is activated. As with all electronic devices, the system should be periodically tested.

## Security/Police Room

In larger trauma centers and hospitals that maintain a fixed security post in the ED, separate rooms or offices are provided for the police and security. In other programs, a single room can be shared. This room should be placed outside the major emergency care activity area. The security/police room provides a place to separate people for taking statements, for detention, and as a place to complete routine reports or to make telephone calls. This room should not be confused with that of an active security post.

## The Hospital Pharmacy

The security of the hospital pharmacy begins with proper handling, supervision, and training of the pharmacy staff. Not all pharmacy employees are honest, and many pharmacy helpers (i.e., pharmacy technicians), cashiers, order clerks, pharmacy students, and pharmacists have been involved in major drug thefts. Personnel hired to work in the pharmacy should be screened thoroughly to establish their integrity. The security department should assist the chief pharmacist and the personnel department in determining the suitability of applicants for these sensitive positions. The Code of Federal Regulations Number 21 (1301.90) covers employee-screening procedures for positions involving controlled substances. Individual states often prescribe additional requirements.

Pharmacy employees are not the only ones who have access to the pharmacy and drug supplies. The environmental services and facilities personnel are often allowed to



move about without supervision and may even be scheduled to clean or to provide maintenance to the pharmacy when it is closed, which is a poor practice.

In addition to environmental services, other employees such as nurses, delivery, and even security personnel should be restricted from having access to areas where drugs are stored. Some states, such as Ohio, require that no individual be alone in a pharmacy unless it is a licensed pharmacist during business hours. In many smaller HCFs, the pharmacy is not open 24 hours a day. In such instances, specific procedures must be developed to detect and document any individual, other than the pharmacist, who enters the pharmacy for emergency purposes.

### Pharmacy Burglary and Robbery

When street drug traffic becomes scarce, pharmacies often become the target of burglary and armed robbery. As retail outlets have become increasingly hardened against attack, and as local pharmacies have become reluctant to include dangerous drugs in their inventories, hospital pharmacies have become a tempting and vulnerable target.

Burglary protection can best be provided by installing proper physical safeguards, such as protection for windows and counter openings, locks, and alarms. Armed robbery presents a somewhat more difficult problem in part because employees often fail to utilize safeguards in place, and in part because many hospital pharmacies fail to install even minimal safeguards.

The major consideration in planning for pharmacy safeguards is to reduce the possibility of personal injury, which is, of course, directly related to avoiding a confrontation. However, confrontations cannot always be avoided, and pharmacy personnel should be trained to respond properly should a holdup occur. Pharmacy robbers are often addicts, excitable, and desperate. Pharmacy employees should obey instructions and avoid any heroics while under observation of the assailant, including activation of an alarm or calling for help. They should note the physical characteristics of the perpetrator and, if possible, the direction of escape. The alarm can be given as soon as it is safe to do so. Employees who remain calm help to avoid triggering violence, and they will be more helpful to security and police investigators in providing a description of the robber and an accurate account of the event.

### Duress Alarms

The use of duress, or holdup, alarms for hospital pharmacies is discouraged. Employees confronted by an armed robber should not do anything that would jeopardize their safety. Organizations should avoid having security or the police respond to the pharmacy during an armed robbery. The telephone should be used to report the robbery when it is safe to do so. If the telephone system is damaged by the perpetrator, the delay in getting to another telephone is generally insignificant.

Those who promote the holdup alarm explain that the security force or the police will not rush to the scene to become part of the problem. Their response should be to take up strategic positions to observe and confront the robbers when they are outside of the

building. This is fine in theory; however, with high turnover and varied police and security personnel, the safest approach for the staff during a robbery in progress is inaction.

Pharmacies that choose to install holdup alarms should make every effort to install them properly to avoid triggering false alarms. The most common mistake in the installation of the panic alarm is to not use a specifically designed activation button, which is recessed to protect against accidental activation. The high rate of false alarms has resulted in the elimination of many previously installed systems. Duress codes may prove a valuable supplement to duress or intrusion alarms. When an alarm is activated and monitored in another location, a telephone call to the pharmacy may be in order. No answer would indicate a possible problem and call for special response procedures. When the telephone is answered, a duress code can be valuable in determining whether a crime is, in fact, being committed and whether employees are in danger.

## Access Controls

The pharmacy work area should be secured so that unauthorized personnel cannot gain unrestricted access. All entrances should be fitted with good locks, and they should be kept locked at all times. To enhance department security, the designated employee entrances should incorporate dual access control technology: card and code, code and biometric reader, etc.

Nonpharmacy personnel, including sales representatives, should not be permitted to freely enter the work areas. Insofar as possible, pharmacies should be windowless. Where windows exist, they should be properly secured and protected by an alarm system.

Openings such as service windows are necessary for the transaction of business. They should be as small as possible, and constructed to preclude anyone being able to gain access to the department. Transaction drawers are preferred to sliding glass openings to eliminate the opening into the department altogether. Most new security designs incorporate bullet-resistant glazing and reinforced steel plating above, under, and around the transaction window and service counter to protect staff against armed weapon penetration. Regardless of the system in place, all should be designed to withstand forced entry. Service windows should also be located so that they are out of the line of sight to access doors. This prevents someone with a gun from ordering an employee to open a door without giving the employee an opportunity to gain protection before reaching the door.

The staff door leading from the pharmacy to the corridor can also present a security vulnerability for exiting pharmacy employees. A robber or thief can wait outside the door for someone to exit. This vulnerability can be reduced with a video surveillance system. The camera is placed in the corridor, and the monitor is placed just inside the door, where employees can see it. Exiting employees can check the monitor before opening the door.

## Closed Pharmacies

Although many hospital pharmacies are open 24 hours a day, others close during the night hours, and often require frequent access by nursing supervisors or other equivalent

positions in the healthcare organization. This access presents a special vulnerability that demands a high degree of personal diligence on the part of the nursing supervisor. In most cases, depending on the frequency of required access and the assessed degree of risk, a security escort should be provided.

An emergency after-hours drug room or large cabinet can also be effective. This container can be stocked with a par value amount of drugs the facility is expected to need that night. This system eliminates many unnecessary trips to the pharmacy. In either case, procedures must be developed to carefully document who enters the pharmacy and what drugs are removed. These records should be available to the pharmacist for review when the pharmacy reopens.

Lights should remain on in the closed pharmacy. The nurse, who goes in and out of the pharmacy, turning lights on and off, informs the intruder that there is only one person to contend with. One pharmacy has entirely eliminated the on-off switch for the overhead lights, so that they remain on all the time and cannot inadvertently be turned off.

Intrusion alarms are highly recommended for all closed pharmacies, regardless of size. Not only are electronic motion detectors and other anti-intrusion devices effective in detecting illegal entry, but they also serve as a strong deterrent to break-ins. Relatively inexpensive holdup cameras can provide additional levels of protection, as well as utilizing video surveillance systems.

## Drug Diversion and Drug Theft

A Dilaudid drip has gone missing. Records show that it had been properly delivered but its whereabouts are unknown and unaccounted for. A pharmacy audit shows a staff member has taken an unusually high amount of narcotics from the automated dispensing machine. An anesthesiologist reports that many patients are complaining of extreme pain after receiving narcotic pain medication. A nurse reports that two syringes of fentanyl and Versed are missing. A charge nurse reports that a patient's bag of fentanyl was empty 5 hours before it should have been. A local retail pharmacy calls, questioning the accuracy of prescriptions for more than 4,000 pain pills.

The theft or diversion of drugs in the healthcare environment is not rare and the examples above are, unfortunately, common reports filed. The National Association of Drug Diversion Investigators (NADDI), a nonprofit organization that facilitates cooperation between law enforcement, healthcare professionals, state regulatory agencies, and pharmaceutical manufacturers in the prevention and investigation of prescription drug diversion, reports that nursing personnel constitute the bulk of drug diversion from HCFs. A study conducted by the NADDI's Cincinnati unit found that a nurse was arrested approximately once per week from healthcare facilities in the Ohio River Valley area for drug diversion.<sup>14</sup> In 2008, a surgical nurse at Boulder Community Hospital in Boulder, CO, was caught stealing fentanyl and replacing it with saline solution. The nurse pilfered more than 50 vials of fentanyl, affecting nearly 300 surgery patients in a matter of months. The nurse was able to steal the medications by ordering through the automated

drug-dispensing machine, then canceling the order after he had removed the drug, injected himself, and replaced it with saline solution. The system was upgraded and now does not allow anyone to cancel a narcotics order. But cases of drug diversion or theft are not limited to just nurses.<sup>15</sup> In 2009, a hospital surgical technician with hepatitis C working at two different HCFs in Colorado stole patient painkillers, and after using, she substituted the drugs with a saline solution in the reused syringe. The case is a rarity as it combined drug diversion and a potentially deadly disease with the surgical technician leaving behind her dirty needle for use on the patient, exposing thousands to her infectious disease.<sup>16</sup> In 2008, a radiology technician working at both Lancaster General Hospital and Heart of Lancaster Hospital in Lancaster, PA, was caught stealing drugs to feed his own habit. The employee was fired, but came back to the facilities many times in the months after his dismissal dressed in scrubs and sharing with any hospital staff that approached him that he forgot his identification badge. Once in the hospital, he would break into biowaste bins and take leftover fentanyl and inject in the employee bathroom.<sup>17</sup>

Fentanyl patches are also a common target of abuse and diversion. The drug is designed to be placed on the pain patient's body and the potent narcotic released over a 3-day period. Abusers may slit the patch open and put the drug under their tongue, use it as a suppository, chew it up and swallow the contents, or apply a heat source to the patch on their body to increase the delivery of the fentanyl. Wasting procedures for fentanyl patches should be closely reviewed and scrutinized. Many HCFs have reported theft of sharps containers due to a drug seeker's desire to obtain wasted fentanyl patches. Experts have estimated that in many instances only 20% of the active drug is used by a patient before it is replaced or disposed of.

HCFs are required by the DEA and other regulatory agencies to carefully secure drugs. The DEA, under the Controlled Substances Act, requires every pharmacy to ensure that there is a closed system of distribution for controlled substances in order to minimize the risk of drugs being diverted and used illegally. The DEA requires registered pharmacies to employ security distribution policies and technology that incorporates authentication, nonrepudiation, and integrity in the record-keeping process. Records of each dispensing must be maintained for 2 years from the date of dispensing of the controlled substance. However, many states require that these records be maintained longer for periods of time. These records must be made available for inspection by the DEA or other authorized investigative agencies.

Today, most organizations have automated dispensing machines that require individual codes or biometric readers (fingerprints, palm, or retina). Many of these electronic systems track narcotic from the time they arrive at the hospital until they are administered to the patient or destroyed. Every healthcare organization using Schedule II–V drugs are required to conduct a daily reconciliation. This activity is almost always performed by the caregivers on the unit and periodically audited by pharmacy staff. Monitoring software is available and used by many healthcare organizations that work with automated dispensing machines to detect unusual usage patterns. At Wake Forest

University Baptist Hospital in Winston-Salem, NC, security/risk management investigators probe each and every discrepancy found in the daily reconciliation and any unusual usage patterns identified.

Organizational policy and frequent reminders for staff are recommended so that staff do not leave drugs unsupervised in surgical suites before the patient arrives. In the case of the surgical technician with hepatitis C, she was caught in an operating room where she was not assigned. Hospital policy forbade the practice but as with most every surgical suite, the practice is commonplace. Fortunately, the hospital policy did allow for her to be immediately drug tested. The healthcare security administrator is often involved in the early investigation of drug theft or diversion. This typically includes working with the chief pharmacist or other designee to review audit trends and possibly conduct initial interviews. HCFs are required to report all incidences of drug diversion to the state health department and law enforcement authorities. The healthcare security administrator should have contact information readily available and assist pharmacy staff or law enforcement authorities as needed.

### *Forged/Altered Prescriptions*

Forged, altered, and bogus prescriptions continue to be a popular source of diversion for the prescription drug abuser. For many years, forgers have used correction fluid to blot out the ink on prescriptions they wanted to change. They would then take this piece of paper to a photocopier and produce what appears to be a blank prescription. The problem with this method is that it requires the forger to write an entirely new prescription. The more popular method today is to use fingernail polish remover for the acetone it contains. Acetone will remove ballpoint pen from paper. Those involved in criminal drug diversion will use acetone to “wash” the prescription. This means the chemical is only used to eliminate the drug they want to change, leaving the doctor’s signature intact. The sought-after drug is then written on the altered prescription, often with no one the wiser, including the pharmacist who ultimately dispenses the drugs.<sup>18</sup>

## References

1. For Healthcare Professionals: Guidelines on Prevention of and Response to Infant Abductions. (2009). *National Center for Missing and Exploited Children* (9th ed.). Arlington, Virginia.
2. Glasson, L., Rozovsky, F., & Gaffney, M. (2007). Security challenges and risk management strategies for child abduction. *Insights*, 12. Retrieved January 4, 2008 from [http://www.onebeaconpro.com/insights/insights\\_vol12.pdf](http://www.onebeaconpro.com/insights/insights_vol12.pdf).
3. Marko, D. (2009). Hospital and police report: How woman tried to steal newborn. Retrieved March 27, 2009 from <http://www.thedailyjournal.com/apps/pbcs.dll/article?AID=/20090327/NEWS01/9032703>. *The Daily Journal*.
4. The Associated Press. (2006). Mother of kidnapped baby released from hospital. Retrieved September 20, 2006 from <http://www.foxnews.com/story/0,2933,214260,00.html>. *FoxNews.com*.
5. Summers, C. (2007, October 27). The women who kill for babies. *BBC News*. Retrieved November 2, 2007 from [http://news.bbc.co.uk/nolpda/ukfs\\_news/hi/newsid\\_6990000/6990419.stm](http://news.bbc.co.uk/nolpda/ukfs_news/hi/newsid_6990000/6990419.stm).

6. The Associated Press. (2008). Arraignment postponed in Kennewick baby case. *The Daily News Online*. Retrieved July 4, 2008 from [http://www.tdn.com/articles/2008/07/02/breaking\\_news/doc486bfe640d742236235014.prt](http://www.tdn.com/articles/2008/07/02/breaking_news/doc486bfe640d742236235014.prt).
7. Aleccia, J. (2008, September 4). Worst nightmare: Babies stolen from their beds. *MSBC.com*. Retrieved September 5, 2008 from <http://www.msnbc.msn.com/id/26532421/print/1/displaymode/1098>.
8. Giordano, M. (2009, January 1). Woman accused of trying to steal newborn at hospital. *The Tennessean*. Retrieved January 3, 2009 from <http://www.tennessean.com/apps/pbcs.dll/article?AID=/20090101/NEWS01/901010348/1006>.
9. Taylor, G., & Finley, G. (2008, March 30). Cops: Woman used ruse to steal baby in Sanford. *Orlando Sentinel.com*. Retrieved March 30, 2008 from [orlandosentinel.com/news/local/seminole/orl-prerelease3008mar30,0,4250897.story](http://orlandosentinel.com/news/local/seminole/orl-prerelease3008mar30,0,4250897.story).
10. The Joint Commission. (2009, January 13). Infant abduction drills. *Frequently Asked Questions*. Retrieved January 31, 2009 from [http://www.jointcommission.org/AccreditationPrograms/Hospitals/Standards/09\\_FAQs/EC/infant\\_ped\\_abduction\\_drills.htm](http://www.jointcommission.org/AccreditationPrograms/Hospitals/Standards/09_FAQs/EC/infant_ped_abduction_drills.htm).
11. Butler, A. (2009, June 22). *Emergency Room Violence: An Everyday Threat*. Presented at International Association for Healthcare Security and Safety Annual General Membership Meeting and Seminar.
12. Emergency Nurses Association. (2007). *Study of Workplace Violence Against Registered Nurses in Emergency Departments*. Retrieved June 8, 2008 from <http://www.ena.org/research/current>.
13. Sarratt, W. G. (2007). Separated only by a common language—communication in the emergency department. *Journal of Healthcare Protection Management*, 23(2), 114–116.
14. Burke, J. (2005). Drug diversion: The scope of the problem. *National Association of Drug Diversion Investigators*. Retrieved July 12, 2009 from [http://associationdatabase.com/aws/NADDI/asset\\_manager/get\\_file/3143/drug\\_diversion\\_the\\_scope\\_of\\_the\\_problem.pdf](http://associationdatabase.com/aws/NADDI/asset_manager/get_file/3143/drug_diversion_the_scope_of_the_problem.pdf).
15. Boulder hospital: Nurse swapped painkiller with saltwater. (2008, November 7). *The Denver Post*. Retrieved November 7, 2008 from [http://www.denverpost.com/breakingnews/ci\\_10920840](http://www.denverpost.com/breakingnews/ci_10920840).
16. Brown, J., & Booth, M. (2009). Hospitals fight inner demons. *The Denver Post*, 1A, 8A.
17. Collin, L. (2007, November 1). Hospital drug arrest. *CBS 21 News*. Retrieved November 5, 2007 from [http://www.whptv.com/news/local/story.aspx?content\\_id=f3dcde80-7813-4f1d-84](http://www.whptv.com/news/local/story.aspx?content_id=f3dcde80-7813-4f1d-84).
18. Burke, J. (2005). Drug diversion: The scope of the problem. *National Association of Drug Diversion Investigators*. Retrieved July 12, 2009 from [http://associationdatabase.com/aws/NADDI/asset\\_manager/get\\_file/3143/drug\\_diversion\\_the\\_scope\\_of\\_the\\_problem.pdf](http://associationdatabase.com/aws/NADDI/asset_manager/get_file/3143/drug_diversion_the_scope_of_the_problem.pdf).

# Areas of Special Concern

*Medical center* is the term commonly used to denote a hospital campus that contains the major inpatient/outpatient services of a healthcare organization. The campus can be a large single-facility structure or a primary facility structure with numerous freestanding buildings. There are various operating functions and services at all medical centers that require the specific attention of security. Not all of these activities will accede to the level of a defined security sensitive area. It is not particularly wrong to classify some of these marginal areas as security sensitive at a specific facility owing to a variety of circumstances. However, an objective of security is to not overclassify an area as sensitive, since the level of protection and added security compliance requirements may impose additional burdens that may not be necessary. It is also important to keep in mind that areas of security special concern, or designated sensitive areas, may change from one category to another category owing to changing risk/vulnerability factors. In this chapter, we will limit our discussion to the main care facility, with the understanding that many of the same special security concerns may be present at a number of off-campus locations.

## Health Information Management

This area of special security concern in the not too distant past was known as *medical records*. The safeguarding of patient information has always been a high priority of healthcare organizations. When patient records were basically maintained as hard copy paper records, the release of information was generally person to person, with telephone and fax transmissions carefully guarded. As the use of fax machines increased, and with the introduction of electronic information systems, the landscape of safeguarding patient information changed dramatically.

The Privacy Act of 1974 was enacted by the federal government to stop the widespread abuse of government information systems. Under the Act, healthcare organizations were prohibited from disclosing information contained in a medical record, except under the following conditions:

- The organization had the patient's consent to release information contained in the medical record.
- The organization was served with a subpoena or court order to disclose the information.

- Public health supersedes the patient's rights, such as in cases involving infectious disease.
- The organization is required by law to report the information to a public agency.

Then in 1996, the often confusing and always changing federal Health Insurance Portability and Accountability Act (HIPAA) was enacted. The act, still not thoroughly understood, has many interpretations and continues to be a major contributor to the increasing cost of healthcare with minimal positive benefits. HIPAA is more fully discussed in *Chapter 1, The Healthcare Environment*.

The primary responsibility for the safeguarding of patient medical information is that of the Director of Health Information Management, the facility privacy officer, and the care providers who are generating and managing the active treatment data on a day-to-day basis. The security program provides support for the protection of this information. This support includes but is not limited to:

- Advising the health information management (HIM) department regarding proper physical security safeguards to include access controls.
- Providing after-hours access to various sections of the HIM department under clear and specific guidelines. All access should be documented and a record of access granted should be forwarded to the HIM director on a daily basis.
- Providing periodic inspections of the access points to the department after hours and provide monitoring of physical security devices.
- Assisting the HIM director in conducting investigations of breeches, or suspected breeches, of information security.
- Fostering a joint working relationship between HIM, security, information technology, and direct care medical providers.

The director of HIM should ensure that strict staff guidelines as well as the physical security safeguards are in place and functioning properly. The security precautions should include:

- Separation of patient medical records concerning cases of litigation or possible future litigation; these records should be maintained by the person in charge of HIM in a secure storage container.
- Establish procedures for HIM and medical care staff after-hours access.
- Tight controls over photocopier use by department employees.
- Built-in safeguards for computerized medical records systems to reduce the possibility that a nursing unit monitor and printer will be used to circumvent normal disclosure procedures.
- A written affidavit signed by medical records employees that they understand disclosure procedures and intend to abide by those procedures.
- Restricted access to medical records during operational and nonoperational periods.



- Physical separation of the doctors' dictating area from the medical records storage and work area.
- A floor-to-ceiling wall partition and/or an intrusion alarm system in the records area.

## Materials Management

The materials management responsibility is defined somewhat differently in each health-care organization. For the purposes of security, the general areas of concern are purchasing and receiving, storage, equipment accountability and marking, distribution, and disposing of property. All of these areas are the responsibility of the Director of Materials Management and require a certain level of security review and support.

### *Purchasing and Receiving*

Because healthcare organizations purchase large amounts of goods, products, and equipment, a proactive loss-prevention program is necessary. A materials management program requires checks and balances and a separation of the staff responsible for purchasing and the staff responsible for receiving. Many opportunities for kickbacks exist in purchasing activities, somewhat in relation to the size of the function; the larger the program, the greater the opportunity, and thus the greater extent of this type of fraud. Not only is the separation of purchasing and receiving necessary, but also the rotation of job assignments is a sound management practice to deter criminal activity. The receiving dock and the process of receiving supplies and equipment present numerous security vulnerabilities. A frequent problem that facilities encounter is that received goods are left unattended on the dock, and thus accessible to delivery drivers or others passing by or through the department. After being checked in and signed for, all goods should immediately be transferred to a using unit or removed to a controlled storage location. A small fenced holding area on the dock may provide temporary protection, pending distribution or transportation to a more permanent storage area. All deliveries to the facility should be directed to a specific receiving area, and the internal distribution of light deliveries, including flowers, should be performed by organizational personnel. Many problems have occurred because delivery personnel were allowed to make their own deliveries to various departments within the organization. These problems include unnecessary traffic, extra housekeeping due to careless handling, interruption of direct or indirect patient care, and the misplacement of material delivered to the wrong location. The delivery of goods and materials by outside service employees continues to grow with the advent of the just-in-time concept of delivery and distribution. This just-in-time concept simply means reduced need for storage and the double or triple handling of supplies, both of which are intended to reduce costs. In this case, cost is reduced at the expense of management control, which, if not managed, can provide the potential for losses greater than the savings.

In a typical large organization, it is common for a semitruck, or two, to arrive at the facility receiving dock at 2 A.M. At this time, the vendor's staff unloads and delivers throughout the house to operating departments and units. This activity, which takes several hours, exposes the facility to access by unwanted persons through the loading dock open access point. The vendor employees, often with questionable hiring verifications, are free to move about the entire facility unsupervised. All of this activity has the potential for serious security consequences. Some just-in-time vendors have been given keys or access cards for free access to the facility. If uninhibited access is provided to contract employees, service agreements with the provider should require that minimal hiring standards be met. Confirmation that the employee meets the minimum standard should be required prior to issuance of keys or access cards. The agreement should also stipulate that ongoing checks are conducted periodically and made available for audit by the organization's human resources department. At minimum, checks should include criminal history, social security verification, and sex offender registry.

### *Storage*

Although general storerooms contain many pilferable items, the losses from these areas are generally minimal compared to the losses that occur after the goods have been distributed to the units. One reason the loss is minimal is because most materials management personnel have recognized the potential for large-volume losses and have implemented at least basic security precautions. All general storerooms should be alarmed after hours, and the sensing devices should transmit a signal to a central alarm panel. Whenever possible, storerooms should be windowless, and the number of access (door) openings should be reduced to the minimum. The system of perimeters is a valid concept for the security of general storeroom operations. Certain areas within the general storeroom should be sectioned off to provide greater protection for particularly vulnerable items, including syringes, blank checks, invoices, and linens. Regular storeroom employees can thus be restricted from areas or access to storage containers to which they do not need access to perform their jobs. Storerooms should be off-limits to all but department personnel. This rule is common, but so is nonenforcement. In one case, employees leaving the workplace were permitted to cut through the storeroom and leave by a side door.

After-hours access to storerooms can present a problem. If the materials management function is properly carried out, there should be little, if any, need for after-hours access. A 600-bed hospital with a firm policy restricting after-hours access recorded only two after-hours entries during a 1-year period. On those two occasions, the storeroom manager had to come from home to provide the access. If entry to the storeroom is necessary, a security officer should accompany the individual to the storeroom. To provide proper accountability, a requisition or record of items removed should be prepared by the security officer for any items taken. The security officer should also be responsible for securing the area when the business is concluded. In this respect, the security officer should be present in the storeroom the entire time another person is allowed entry after regular hours.

### *Equipment Accountability and Marking*

A common practice in healthcare organizations is to receive a piece of equipment, assign an asset control number to it, affix the number to the equipment, assign a depreciation schedule, and deliver the equipment to the requesting department—never to see it again. For example, a computer acquired for the public relations department may end up in the nursing office, and the new location will not be recorded. After these transfers have been made several times, the computer's location cannot be readily established and may indeed be missing. Equipment should be assigned to a specific department, and a periodic inventory is essential. When property is transferred, the record should be annotated to relieve one department and assign accountability to the other. Related to the assigning of asset numbers—and of equal importance—is marking property with organizational identification. “Marking” refers to conspicuous identification that cannot be easily altered or removed. Many items must be marked with more than the asset control number. When marking equipment to deter theft, basic economics must be considered. A balance must be found between the cost of marking and the actual theft deterrent value achieved. Not all markings need to be readily seen. For example, desks, file cabinets, tables, and chairs should be marked on the underside, permitting ready identification but not defacing the appearance of the property. Furniture is normally stenciled with the hospital's initials or logo. Etching tools are used for instruments and other metal equipment.

### *Distribution*

The distribution of goods and equipment from storage areas to end users is accomplished by walk-up distribution counters or transported to the user by materials management personnel. The latter method is being utilized more frequently as off-site storage areas are becoming common. Regardless of the distribution method, all supplies and equipment should be signed for by an authorized staff person at the point of delivery. The person signing for the property must take time to determine that the property being signed for is actually delivered. When staff simply signs a receipt without checking, it is an open invitation to receive a short delivery with property being fraudulently diverted. At this point, the delivered property should immediately be properly stored and not exposed to passing staff or visitors.

## **Disposing of Property**

All healthcare organizations accumulate and need to dispose of obsolete, excess, or damaged property. Organization staff, including the supervisory staff, should not have the authority to give away or otherwise dispose of facility property, regardless of its value. A firm policy should be established that outlines the authorized disposition of unneeded property through the materials management department. All unneeded material should be transported to a central storage area so that it can possibly be used by another department. Thus, property may be reassigned and properly managed. Healthcare facilities are notorious for needlessly purchasing an item because no one knew the same item

was no longer needed by another department. A committee—composed of the Director of Facilities, the materials manager, and other administrators—should periodically survey the material in storage to determine what should be discarded. A sale, accessible to employees only, is a good employee-relations mechanism that can eliminate the practice of giving away property to “favorite staff,” which can result in negative employee relations.

## Laundry and Linen Control

The loss of linens in medical facilities of all sizes has generally gone unchecked, and it continues to needlessly increase the cost of patient care. Too many administrators and laundry managers believe that satisfying unit needs is more important than trying to halt linen thefts and misuse. The theft of surgical scrub suits has attracted press coverage, which has prompted some administrators to alter methods of control. However, little has been done to reduce shrinkage, giving the impression that the problem is not a major concern—neither too bad or it will go away with time. Security practitioners must understand why it is so difficult to focus the attention of laundry personnel and hospital administrators on laundry theft and misuse. First, “more linen” has erroneously been translated into “better patient care.” Second, many administrators falsely believe that increased linen use reduces the cost per pound of processed linen. Laundry managers in general take great pride in reducing cost per pound, rather than in reducing use. The cost of linen service should be measured in cost per patient day to be meaningful.

The term *linen control* should also be examined. Most hospitals operate supply systems rather than control systems. The basis of a supply system is often to establish a quota for each item for each unit, often referred to as a *par value*. Supplying the units is only part of a control system; the soiled linen returned from the unit must also be accounted for. This control must be in place whether the facility processes their own laundry or contracts with an outside vendor for such services.

## Establishing Losses

Linen loss figures are difficult to establish unless strong procedural controls and adequate recording methods are instituted and maintained. One method of determining a loss in the supply system is to review the amount of linen put into the system after adjusting for the amount of linen discarded. These numbers must be viewed over a period of time because input varies over the year. Excessive amounts of linen added to the system is often rationalized by suggesting that inventories were increased owing to extremely hot or extremely cold weather, a higher census, exceptional medical cases that required more frequent changes, hoarding by units, and the like. These explanations may have limited merit; however, a review of trends over a longer period of time generally indicates whether losses are in fact occurring. A complete review of the movement of linen, from ordering to the end user, and the reprocessing system is the first step in establishing a linen security program. Security practitioners and laundry administrators must examine

each step of this process to note the controls that are in place and to identify areas of possible compromise.

### *Controlling Losses*

Most institutions find it difficult to pinpoint the specific areas in which linen loss occurs. In a shared laundry, the user facility causing the problem can also be difficult to identify. This leads to such generalized security efforts and safeguards that the linen thieves are rarely threatened by them. When losses occur, the basic problem is that the linen processing system is not a closed-loop system. The amount of soiled linen returned by each department, or hospital, is not determined. The problems that result would be similar to those of a car rental agency that never checked whether cars were returned. The only way to continue to rent out cars would be to purchase a new one for every one that was not returned. Unfortunately, this seems to be the manner in which many hospitals operate in terms of linen replacement. To combat these problems, a number of shared laundries and a few large in-hospital laundries have commenced soiled linen-counting systems, which are much more accurate than weight accountability. These systems return clean linen to the units on the basis of the amount of soiled linen that was returned. The laundry replaces the linen that wears out normally, and when a unit requires new linen, it is charged directly to the unit. Healthcare facilities personnel are not disposed to inventory routines. In view of the serious problem of linen theft, however, healthcare facilities should conduct at least one complete inventory each year. Several inventories per year are highly recommended when a linen disappearance problem is suspected or there is an actual occurrence of a substantial loss. Not all linen losses are attributed to theft. Some losses occur through waste and misuse. Employees who wipe up a spill with a washcloth and throw it into the trash or who tear up linen for rags can produce a significant loss problem. The discarding of linen should be a controlled practice, and the transformation of discarded linen into rags should be a centralized operation. Rags should be appropriately dyed a specific color and supplied to users to prevent abuse of the reusable linen supply. New linen that has not yet been put into the system should not be stored in the laundry area. New linen should be maintained in the general storeroom and dispersed to the laundry operation through a regular requisition system.

A long standing observation by security personnel is the common practice of EMS units and private ambulance services to help themselves to clean hospital linen in exchange for the soiled linen they leave behind after a transfer. The problem with this exchange is taking two or three of the clean linens versus what they leave. One of the “tongue in cheek” comments by those who witness such transactions is that the ambulance company has been in business for 10 years, but never bought or laundered a single piece of linen.

### *Scrubs*

More has been written on the loss of hospital scrub suits than on the rest of the linen theft problem. Scrub suits seem to appeal to all segments of the population, from teenagers to college professors. Some predict the scrub suit trend will continue indefinitely, but

others feel it is probably just a passing fad. Whatever the future holds, the public's love of scrub suits has cost hospitals millions of dollars. The solution to this type of loss is quite simple. First, scrub suits should be issued to individuals. A soiled suit can be exchanged for a clean suit either through an issue window during set hours or through an automatic uniform dispenser. This is another use for access control ID cards. The second step for simple scrub suit control is an administrative directive with real support. Hospital property should never leave the premises, and violators should be firmly dealt with rather than ignored. An even better method of control is the growing practice of requiring staff to furnish their own scrub attire.

#### *Access Controls for the Laundry*

The laundry itself must be provided with good after-hours physical controls. These safeguards include strict access control, which often include an intrusion alarm system. Personnel should not be permitted to enter the laundry to supplement inadequate unit inventories. Once the laundry is closed for the day, it should remain closed, just like the pharmacy, food service, and the general storeroom. To meet unexpected emergencies that require extra linen, one method is to provide a small emergency supply in another area. For example, a fully stocked linen cart can be placed in a locked closet that is accessible only to a nursing supervisor. This emergency cart could also be stored in central supply if this area is operational 24 hours a day.

#### *Marking Linens*

Materials management personnel should be responsible for marking linen with the facility's name before releasing it to the laundry. Linen can be ordered from vendors with the hospital's markings; however, many hospitals buy unmarked linen and perform this task themselves. All linen, with the possible exception of washcloths, should be marked. Sheets and other large items should be marked in at least three places, on opposite ends, and in the middle of the item. Despite some claims to the contrary, marking linen does deter theft. Marking is an important step in the total control system, and it is essential for pursuing arrests and prosecution when thefts occur.

### **The Research Laboratory (Animal)**

The activities of animal rights groups and antivivisectionists, responsible for acts of eco-terrorism, have made laboratory security a high priority for facilities conducting animal research projects. These rights groups are often well financed and can be very sophisticated and frequently benefit from the attention of a sympathetic media. One of the best-known groups is the Animal Liberation Front (ALF). Research facilities in hospitals, universities, and independent firms have been the target of demonstrations, break-ins, vandalism, and fires. In one case, more than 1,200 laboratory animals were released just before two university laboratory buildings were set on fire. The ALF claimed responsibility for these acts. In addition to physical damage, graffiti, and disruption of normal work, pressure by animal rights activists can result in the suppression of important research.

There are also a growing number of incidents and concerns relative to threats facing researchers and their families. The defense against ecoterrorism requires planning for both perimeter security and the protection of the contents of the laboratory: animals, equipment, records, and personnel.

### *Employee Background Checks*

When the security of sensitive projects is involved, it is of prime importance to know laboratory employees well, through background-verification procedures. Information provided by an employee who is sympathetic to the animal rights movement can allow activists to gain access through even the most efficient security system. The animal rights activist movement goes back several hundred years in Europe and expanded to the United States well over 100 years ago. In the past 5 years, the activist groups have become more active, and somewhat more radical. The new leaders are young, confrontational, and dissatisfied with the lack of progress. As a result, they advocate more direct action that leads to violence and destruction of property. According to Debra Higgins Cavalier, president of the Massachusetts Society for Medical Research (MSMR), there are well over 70 animal activists groups in the United States. The MSMR is one of the leading nonprofit groups in the United States that support the bioscience in the proper use of animals in research. Massachusetts was the first of several states to enact legislation making it a felony to trespass upon, remove, damage, or interfere with any property used in animal research. There is also the Federal Animal Enterprise Protection Act of 1992 that makes it a felony to break into a laboratory and cause damage in excess of \$10,000.<sup>1</sup>

### *Activist Methods of Infiltration*

The ALF distributes handouts to supply operatives with tactical information. One such handout recommends eight methods of gathering information on targeted institutions. These methods are:

- *Personal entry.* In this method, the operative simply walks into the facility. If challenged, the operative simply states he is looking for a friend.
- *Employment.* In this method, the operative gains employment at the targeted facility.
- *Use of disguise.* In this method, the operative impersonates a government employee, inspector, etc.
- *Surveillance.* In this method, the operative conducts a fixed surveillance (stakeout) of the facility.
- *Use of inside help.* In this method, the operative develops friendships with facility staff.
- *Bribery.* In this method, the operative bribes facility staff.
- *Garbage inspection.* In this method, the operative inspects the target's garbage.
- *Surreptitious entry.* In this method, the operative gains access to the facility surreptitiously. Lab coats, required safety equipment, and badges help to identify authorized employees during normal working hours, but identification can be difficult after hours.<sup>1</sup>

Animal activists have preferred holidays and early morning hours for break-ins, so security personnel should make sure that doors, windows, and all other possible entries are locked at the beginning and end of each workday and immediately after the last employee has left. In addition, visitors should be restricted from sensitive areas, repair people should be carefully identified, and reliable alarm systems used. Because intruders often disable power substations—thus cutting off electricity to the research facility—an emergency power system is advisable for lighting, preserving specimens and agents, and maintaining animal life-support systems.

## Child Development Centers

It is somewhat common for healthcare organizations to operate a child development center, or childcare center, as a means to attract and retain physicians, staff, and employees. These centers present unique security concerns. The first and primary security concern is the development of appropriate staff. Intense background checks of applicants must be conducted; certain checks are even legally mandated by regulatory and licensing agencies. The sexual molestation, or other physical abuse, of a child by a staff member is a situation to be prevented at all costs. Limiting access to the facility is also a primary safeguard. It is a common practice to have all ingress/egress points locked except for the normal drop-off and pick-up times. Some facilities maintain a locked facility at all times, issuing electronic access cards to authorized family members only. An outside play area is generally a design feature of the child development center. These play areas should be completely fenced with at least 6-foot-high barriers. The normal access to the area should be from the daycare center itself. If there is a gate arrangement, it should be locked from the ingress side and the release side (egress) should be such that small children cannot operate the release. Staff personnel should be especially watchful for persons loitering in the area around the center. Release of a child at the end of the designated time period is an area of special concern. First, there is generally a lot of activity going on during the pick-up time, resulting in difficulty of keeping track of who is coming and going. Second, there must be strict criteria established regarding the identity of persons who can pick up a child. There must be a system to permit the release of a child to someone other than a normal family member due to a family emergency or other extenuating circumstances. Regardless of the policy and resultant procedure, there should be strict adherence to this critical element of security. Video surveillance has several appropriate applications to help secure a childcare center. In addition to surveillance of general areas, a camera should be placed at the main access door to record the dropping off and picking up of the children. In some cases, this will require two cameras to adequately record the activity. As with all other video surveillance applications, the recorded video should be kept for a specified time period, which is documented in a written policy and procedure. The video system may also be used to allow the remote electrical release of the main entry door from a remote location. The general security plan for a childcare center should include procedures for relocation of children and staff in the event of an emergency requiring



evacuation. This information should be given to parents at the time of enrollment. It can be included in an overall security-briefing card that is a standard handout to parents, outlining operating procedures and expectations of the parent/guardian.

## Business Office/Cashiers

Business offices and cashiers are part of the operating environment of most healthcare provider organizations. Although the activities assigned to the business office, and the specifics of cashiering, will vary from organization to organization, they present a security risk. These risks and resulting security safeguards should be a collaborative effort of security and the appropriate department administrator.

The greatest loss risk in performing these functions is the employees themselves. While robbery and theft by outsiders do happen, the frequency and risk of such incidents in the healthcare environment is fairly low. At the close of a cashier function, or changing of shifts (i.e., cafeteria), receipts should be taken to the designated central cash management location for accounting and storage. There needs to be a night/weekend drop safe or device of some sort for after hour delivery and storage of receipts and, in some cases, patient valuables. The physical security of the drop mechanism and storage container should be of substantial construction. The drop usually takes place in a hallway or corridor, with the storage container on the other side of the wall in a secured area. A video surveillance system should provide a clear image of all persons, and their actions, in and around the drop area. It may take more than one camera, as a wall may preclude getting a full face-shot of persons facing the actual drop.

Persons transporting receipt bags from an operating unit should utilize a locked bag. In this respect, the transporter should not have the ability to access the contents of the bag. Many such bags involve a double lock-type system of control. It is also somewhat common for a security officer to provide a cash escort for certain transports, or to have two general staff persons complete the transfer. Most outsourced security companies cannot obtain liability insurance coverage for internal theft or robbery during a cash escort. The cash receipts are also not protected by the typical crime policy held by most facilities. As a result, these security staff members should escort a facility employee and not be requested to conduct cash escorts alone. It is suggested that cash transfers that require the leaving of a building and traveling any distance on the grounds be accomplished by two persons. An armored car service is a standard security requirement for community banking services, except in the very small communities where no such service is available.

## Information Technology

There have perhaps been more compromises of healthcare information in the 2-year span of 2008–2009 than the total compromises of the previous 10 years (1997–2007). Data breaches grab headlines on almost a daily basis. Healthcare providers maintain data

ranging from a person's credit card numbers, social security numbers, credit ratings, to the most private and intimate health details. The lack of coordination among physical, privacy, and virtual security personnel has been part of the problem. As a result of this disconnect of parties, the term *convergence* has been coined. There are various definitions of convergence; however, in simple terms, it means getting IT people and security people working together in an effective working relationship. The common elements of convergence are running physical security systems over network wires, common credentials for door and logical access, and integrated logical and physical applications.

There are many technologies used for the transmission of information in health-care, many of which carry sensitive medical and personal information. Wi-fi and wireless technologies are widely deployed technologies in the healthcare environment but are both prone to hacking as security safeguards for the most part are still in their infancy.

Mobile technology is of immense value to healthcare professionals; however, the security threats in these technologies create much concern. The US Department of Health and Human Services (HHS) published guidance in 2009 that outlines the ways that health information can be protected from security breaches. It builds on rules in the HIPAA. The guidance is connected to two future breach notification regulations, one that will be issued by the HHS and the other by the Federal Trade Commission for vendors of personal records and those entities not covered by HIPAA. HHS guidance describes several technology solutions for security breaches that would make personal health information "unusable, unreadable or indecipherable," as the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act requires.<sup>2</sup>

The security staff can assist the IT unit in physically hardening the space utilized by IT with access control, alarms, and video surveillance. Security can support IT by helping to secure mobile data devices to collect patient data, access data, and signal caregivers. The array of easily lost or stolen devices and media includes PDAs, laptops, CDs, DVDs, flash and thumb drives, as well as data cards. The security of software protection, firewalls, etc. is largely in the domain of the IT staff.

Server areas and other sensitive equipment locations should be secured. Vendors, repair persons, and other persons not assigned to these areas should be tightly controlled. A system of badging, logging in and out, and escort procedures should be part of all IT security plans and systems.

Physical security safeguards, however, cannot prevent internal breaches by those in a position of trust. On July 1, 2009, a security officer at the Carrell Clinic in Dallas, TX, was taken into custody after taking complete control of computers that administered the facility's air-conditioning systems. The security officer had no authorized access to health system computers but was able to hack into the network controller and physically inactivate all internal alarms.<sup>3</sup> Many elements of critical infrastructure, like environmental controls in most healthcare facilities, have low security and are prone to even low-skilled attackers.

To enhance the awareness among public hospital staff in protection of personal data of patients, the Hospital Authority in Hong Kong and the Office of Privacy Commissioner for Personal Data (PCPD) launched the "Care for Patients—Protect Their Personal Data" campaign. Through a series of training seminars on the Personal Data (Privacy)

Ordinance, with interactive games and exhibitions, the campaign is aimed at strengthening the culture of privacy awareness in the daily routine of hospital staff with particular attention to preventing the loss and possible leakage of patients' personal data. Likewise, the PCPD designed an online self-learning program to facilitate the training of healthcare workers on the protection of personal data.<sup>4</sup>

## Intensive Care Units

The ICU is an area that is frequently the scene of serious security incidents, from disturbances to homicides. The ICU has the potential to be a highly charged atmosphere at any given time. Another security risk factor is often the high security–risk patient who entered the emergency department for treatment of injuries from a felonious assault, who is then transferred to surgery and on to the ICU. A prolonged stay in the ICU provides an opportunity for a gang member, drug dealer, or others to finish the job. It is becoming more prevalent to restrict access to ICUs at least for certain hours and to provide for a certain level of stationary security. Regardless of how open a philosophy of managing the ICU is, with no routine locking, the capability to lock down the unit in an emergency should be in place.

## Gift Shops

The majority of hospitals have a gift shop staffed for the most part by volunteers. In larger facilities, it is common for the facility to hire an employee as the gift shop manager. The gift shop is a frequent customer of the security department for a variety of reasons, with shoplifting, or suspected shoplifting, the most common need for service. Perhaps the best method of mitigating the shoplifting problem is proper layout of the gift shop, providing clear lines of sight and sufficient staff to provide a clear presence and general surveillance capability.

Gift shops should have basic physical security safeguards in place. These safeguards include card access, video surveillance, mirrors, and an intrusion alarm system. In addition, some shops have elected to install panic alarms, usually connected directly to security. Not all security administrators subscribe to the use of panic alarms in gift shops for several reasons. A primary reason for this lack of support is that gift shop personnel are often responsible for an inordinate number of accidental or unnecessary alarm activations. Second, historical data support the general lack of security incidents when the gift shop is open, with the exception of shoplifting. The use of the telephone to request security services would generally not put the caller in an undue personal risk situation. The configuration of most gift shops provides for a “back room area” from which a call to security can be made in relative privacy.

## Compressed Medical Gases

There are two medical gases of special security concern. The first is oxygen (O<sub>2</sub>) and specifically the central oxygen storage tank that supplies piped-in oxygen to the facility. The security concern is that sabotage or outright destruction of the main hospital storage system

would basically shut down the large hospital facility. Substituting portable oxygen cylinders would be almost impossible in regard to furnishing equipment valves and the other logistics involved.

The second medical gas of concern is that of nitrous oxide ( $N_2O$ ). This concern relates to the theft and misuse of the gas. The major legitimate users of  $N_2O$  are the providers of healthcare. Healthcare accounts for approximately 90% of the market for this type of compressed gas, with dentists using more of this gas than hospitals.

## Main Oxygen Storage Tank

The main hospital oxygen storage tanks at our nation's hospitals generally receive less than adequate protection, and are usually located in a rather prominent and easily accessible location on the campus. A typical level of protection for this tank is a chain link fence that is too short with a padlock at the entry gate. If one could not crawl over the fence, a bolt cutter would easily cut through the fencing and most locks. Security considerations for central  $O_2$  storage tank systems should include:

- Steel/iron fencing of at least 8 feet in height with the base embedded in concrete. A 7-foot fence with barbed wire outriggers or concertina rolled barbed wire would be adequate; however, the aesthetics may not pass administration or some city/county ordinances.
- Night lighting of the area.
- Video surveillance.
- Strict access control, including card access with magnetic locking of 1,000 lbs. or higher.

## Nitrous Oxide Tank Storage

The abuse of  $N_2O$  as an inhalant has increased over the past few years. The illicit market for this gas has been especially popular at concert venues and college campuses. The illicit dealer typically fills balloons with the gas. The gas displaces air. As the inhaled gas concentration approaches 100%, the user achieves a brief sense of euphoria. Within seconds of reaching a 100% concentration of  $N_2O$  in the lungs, a person can stop breathing because of the depression of the central nervous system caused by  $N_2O$  in the user's lungs.<sup>5</sup>

The  $N_2O$  gas is generally stored in cylinders ranging in size from approximately 2 feet in height to over 5 feet in height. The storage of these cylinders requires a locked and tightly controlled level of access. It is important to store empty cylinders with the same level of security, as the residual amount left in the cylinder is also the subject of theft and abuse.

A Florida hospital experienced an incident in which four young persons stole a cylinder of  $N_2O$  from the hospital gas storage area. The cylinder was opened in a vehicle with the windows closed. The result was that one of the four persons died from the inhalation of the gas.

## Food Service

Healthcare organizations, big and small, serve food every day to a large number of patients, staff, and visitors. The process of purchasing, storing, and preparing food products in such large volumes presents a wide array of opportunities for theft and misuse. The management and supervision of the theft problem, of course, belong to the food service department. Security will often be called upon to support the various food service departments' security controls in terms of monitoring and investigating losses. As with many other operating departments, the implementation of a strict access control plan is absolutely necessary.

## Roof Areas

An often-overlooked area of access control is the healthcare facility roof area. Each year, there are patient deaths reported due to either falling off, or jumping, from hospital roofs. In most of these cases, the roof access points have not been controlled properly. Patients can become disoriented owing to a number of medical treatment regimens, and the issue of dementia is a major element of patient safety management. These roof accidents have involved both the inpatient and the outpatient. At one large, mid western hospital, an outpatient of the dental clinic accessed the roof and fell to his death. He had been sent from the clinic to the pharmacy to get a prescription filled. At some point, he lost his way and ended up in a building fire stairway. Once in the stairway, the only way out was the ground level. All ingress to the building from the stairway at all other levels was locked off. Instead of going down, the patient went up, eventually exiting on the roof through an unsecured roof hatch.

In another case, a hospital patient on a regular medical/surgery floor was missing from his bed in the middle of the night. An immediate search of the hospital failed to locate the patient, who was in a hospital gown, as evidenced by his clothing being left in the room. The patient was found the next day where he had apparently fallen from the roof of the multilevel facility.

All roof access points must be locked 24 hours per day. The added protection of alarms and video surveillance is strongly recommended. In one instance, the local fire department insisted that a roof door required the free access of the fire department. In this particular case, the issue was resolved by installing a "Knox Box" at the door that permitted entry by the fire department. More than 9,000 US fire departments, EMTs, and government agencies use the Knox key box system.

## Security Areas of Concern Specific to the Organization

In this chapter, we have briefly discussed some of the more obvious areas of security concern of the security administrator. There are countless other areas that security must evaluate and support, such as front-desk reception, outpatient clinics, therapy units, satellite pharmacies, and such. As the healthcare organizations add and delete specific

services, and reallocate space, there is a need for constant security risk assessment and changes in the delivery of security services.

## References

1. Renewed violence by animal rights activists who target research labs. (1999). *Hospital Security and Safety Management*, 20(4), 13–14.
2. Robinson, B. (2009, April 20). *HHS Offers Health IT Privacy Guidelines*. Retrieved April 27, 2009, from <http://govhealthit.com/Articles/2009/04/20/Health-IT-privacy-guidelines.aspx?p=1>.
3. Goodin, D. (2009, July 1). Feds: Hospital hacker's "massive" DDoS averted. *The Register*. Retrieved July 3, 2009 from [http://www.theregister.co.uk/2009/07/01/hospital\\_hacker\\_arrested](http://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested).
4. Ko, C. (2009, May 8). HK hospital authority steps up patient data security. *Computerworld*. Retrieved May 8, 2009, from <http://news.idg.no/cw/art.cfm?id=21CB162A-1A64-67EA-E489C05803968C27>.
5. Nitrous oxide issues and incidence of abuse. *Compressed Gas Association Foundation Website*. Retrieved November 6, 1997, from <http://cganet.com/page37.htm>.

## Off-Campus Considerations

In this chapter, the main focus of discussion pertains to security of medical center facilities that are not located on the main campus. It should be noted, however, that there are thousands of private patient care facilities that also have security risks that require various elements of security protection. These private organizations, such as physicians' offices, surgery centers, dentists' offices, rehabilitation services, and the like, face the potential of experiencing major security incidents. Physicians being assaulted in their offices and even murdered are all-too-frequent occurrences. In June 2009, Dr. George Tiller was shot to death at his church by a gunman who was apparently upset that Dr. Tiller performed late-term abortions. Antiabortion terrorism and violence have resulted in the killing of three other physicians since 1993. It is reported that following the homicide of Dr. Tiller, US marshals were dispatched to protect doctors and clinics that may have been at risk.<sup>1</sup>

### The Need for Off-Campus Facilities and Services

In today's delivery of healthcare services, more and more healthcare organizations are expanding their medical care programs beyond the main medical center campus. The rationale for some of this expansion is to bring certain care programs to different communities and neighborhoods, to build market share, and to make care more accessible and convenient for the patient. On the contrary, some treatment programs and facilities have been moved off campus as the result of new or growing treatment programs that require additional space on the main campus. One such solution to creating more space for these expanding needs is to move certain functions or services off campus that do not need basic diagnostic or clinical support, which is only available at the main facility. Examples of healthcare treatment programs that can function as stand-alone units are different types of therapy, urgent care centers, sleep clinics, dental clinics, and routine medical checkup and preventive medicine clinics.

An example of a healthcare organization with multiple off-campus locations is the highly acclaimed The Children's Hospital (TCH) located in Aurora, Colorado. Their off-site patient service units are principally located throughout the Denver metropolitan area, with one facility located as far away as Pueblo, Colorado, which is 90 miles from Denver. These facilities collectively are referred to as The Children's Hospital Network of Care. The network currently consists of 12 operating treatment centers ranging from

a small daytime therapy care unit to 24-hour care centers. TCH has been developing a coordinated and integrated security program for these network facilities through the efforts of the corporate Project and Property Manager, who is especially knowledgeable relative to security requirements for such facilities. While there is always work to be done, and new goals being formulated, the TCH manager has provided leadership toward providing a high level of security in protecting patients, staff, and property as an efficient and coordinated systems approach.

Nonclinical healthcare departments or functions are also prime candidates to be moved off campus to create additional clinical space or to occupy less-expensive space. Examples of such support departments, or programs, are staff training facilities, certain Human Resource functions, planning and marketing, accounting, and general supply storage areas. One of the drawbacks to locating some of these support functions off campus is the logistics of moving staff back and forth between the main campus and the off-campus locations. This staff logistical transportation problem, at least to some degree, does not exist when the off-campus service is in the same neighborhood as the clinical care facility. These patient care clinical services do require a well-organized and planned courier and supply service; however, staff does not have a general need to access the main facility on a routine basis.

### Off-Campus Security Risk Assessments

The assessment of security needs and concerns for off-campus facilities, whether down the block or many miles away from the main facility, begins with a site inspection of the existing building and/or the review of new construction or renovation plans. Facilities should use the same approach and information sources as when conducting the main facility security risk assessment. An additional element of review for lease space functions is to determine the security safeguards provided by the property owner as part of the lease agreement. All too often, these off-campus facilities are left on their own relative to security issues until a problem develops. The main facility security resources are then called upon to provide security. These off-campus facilities should be a part of the main facility security program in all respects, with the exception of critical incident response. In an emergency, a public safety agency would likely be the first responder. In terms of communications, all incident reporting and physical security (including key and access control) should be handled as if the off-campus facility were a functional unit within the main facility.

### Home Healthcare (Community Provider Services)

A major off-campus medical care service that does not require space (beyond minimal administrative space), yet is becoming big business with a whole set of unique healthcare security issues, is home healthcare. The delivery of home healthcare services had its beginning in the early 1990s and grew quickly through the mid-1990s. Today, many hospitals and private agencies (both profit and nonprofit) are examining the future and the



direction of their services. There is clear distinction between home healthcare and home care. Even in home healthcare, the definitions of service and the caregiver are not consistent or clear. In terms of state regulation, there are states that regulate home healthcare but not home care. States vary to a great degree on how they regulate the whole issue of home care, with Florida being one of the more progressive states in this regard.

The home environment sets up a new and different relationship between the caregiver and the patient. The patient is now in his or her familiar surroundings, while the caregiver is providing services outside the familiar organizational setting. This change of relationship and environment creates a whole different set of security issues and concerns for the patient, the caregiver, and the organization the caregiver represents. The IAHSS has created a basic industry guideline to help protect staff who provide home healthcare security.

#### IAHSS—HEALTHCARE BASIC SECURITY GUIDELINE, #02.06

##### **Home Health Security**

**STATEMENT:** Healthcare facilities (HCFs) or healthcare organizations (HCOs) providing home health services will develop a security plan to protect staff traveling into the community in the performance of their duties.

##### **INTENT:**

- a. HCFs/HCOs should have a risk assessment process in place which would allow home health staff to determine appropriate safeguards associated with a community visit. The risk assessment process may include a community crime assessment, previous history of the client, and other related factors.
- b. Home health staff should be provided with education and training regarding risk identification and preventative safeguards. Training should include information and guidelines on security awareness, crime prevention, and defensive measures. Training records should be maintained.
- c. HCFs/HCOs should develop a communication process to protect home health staff. This should include proactive check-in and checkout procedures that would allow staff to make contact during the shift to help ensure their safety. Cell phones, automated check-in procedures, or GPS devices may be considered as appropriate, to facilitate this process.
- d. Security personnel or appropriate escorts should be available to home health staff providing services in areas or situations deemed high risk or as individual situations warrant.
- e. Procedures should be in place for home health care staff to follow in the event of a security incident or a situation in which they have a concern for their safety or well-being.
- f. HCFs/HCOs shall have a process in place for responding to incidents or missed check-ins.

**Approved:** June 2008

**Last Revised:** October 2008

### *Patient at Risk*

The caregiver is relatively independent of organizational supervision while in the home. Oftentimes, the patient cannot ambulate and therefore cannot provide a normal degree of surveillance of this stranger in their home. This degree of caregiver independence can lead to a variety of security issues, including:

- Theft of patient property
- Diversion of drugs
- Verbal and physical abuse toward the patient

In one case, a home health aide was hired through After-Care Professional Nurses Registry of California to care for a 96-year-old person. Little did the family know that the caregiver was on probation after serving 8 months for stealing more than \$500,000 from two other people who had been in her care. In fact, the family only learned of the past conviction after filing a police report regarding their own theft of property by the aide. The firm was not a licensed home care agency because it called itself a registry instead of an agency. This firm was listed in the telephone directory as “Home Health Services” and was recommended by local hospitals.<sup>2</sup> A study of 150 cases from 32 states in which home care providers were found to have abused, neglected, or stolen from patients was conducted by *USA Today*.<sup>3</sup> Results of the study revealed that 73% of these cases involved theft, 19% involved violence (including murder and sexual abuse), and 15% involved behavior that put the patient at risk of physical injury. Nurses were involved in 6% of these cases with the remaining 94% involving healthcare aides.

### *Caregiver at Risk*

The caregiver providing home healthcare is subject to a variety of risks in performing services, including:

- Automobile accidents
- Automobile theft and vandalism
- Attack by vicious animals
- Attack by the patient, family, or others present in the home
- Attack by neighbors or persons in the neighborhood
- False accusations including patient abuse and theft of property

In August of 1996, a nurse on a home healthcare visit was shot and killed by a patient who then shot himself. The patient’s sister had warned the nurse that she should leave owing to the mood of the patient following a change of dressings the previous evening. The nurse followed this advice, but forgot her nurse’s bag. The nurse was waiting outside while the sister retrieved the bag. The patient came out of another door and confronted the nurse, killing her and himself.<sup>4</sup> In another case that occurred in February 2000, a home healthcare nurse in rural Kansas was shot and killed while dialing 911 to report finding two bodies on the floor of a client’s home. The nurse was apparently killed by the client’s 23-year-old grandson, who was arrested at the scene for killing his father, another woman at the home, and the nurse. The client (patient) was unharmed.<sup>5</sup>

There have been many cases in which family members or friends have stolen property from a patient and then accused the caregiver of being responsible for the loss. This type of false accusation is particularly true when it involves cash, jewelry, and antiques. The tendency for interfamily theft is quite prevalent when a patient is near death and family members are concerned about getting their fair share of the estate.

### *Security Practices and Guidelines*

There are a number of security practices and guidelines that should be taken into consideration with regards to home healthcare.

*Initial assessment of the home environment.* Prior to the first home health visit, the agency should complete an environment assessment either by direct verbal conversation or telephone contact with the patient or close family member. This assessment should include inquiring about animals, other persons living in the home, medications, neighborhood crime/gang activity, and complete directions for finding the address and accessing the living unit.

*First visit.* If the initial assessment of the home environment presents significant danger signals, there should perhaps be two caregivers making the first visit. This practice is difficult owing to funding issues; however, the safety of the caregiver must take precedence over cost. During the first visit, the caregiver should make an assessment relative to safety or other potential problems presented by the environment. This information should be noted in agency files for further references or for immediate follow-up. For example, should the patient or family openly display or talk about firearms, a safety awareness response is necessary.

*Scheduling visits.* It is always best to schedule home visits during daylight hours. This is not always possible, but should always be a goal. Physicians can sometimes regulate specified times of treatment when they are aware of caregiver safety issues. It is always a good idea to telephone the patient just before the visit as a courtesy and to find out whether there is some legitimate reason to reschedule the visit.

*Preparing for the visit.* Always wear name badges and uniforms that clearly identify the healthcare agency. A cell phone or two-way radio should always be part of the standard equipment carried into the patient's home. Caregivers should always leave supplies, equipment, and personal property not needed for the specific visit in the trunk of their vehicle. Vehicles should always be locked.

*During the visit.* Caregivers should always spend only the time necessary in a patient's home. Instincts are to be trusted and care should be terminated when danger signals are perceived. Suspending treatment is somewhat different than abandonment of care. Immediate termination of care is justified if there is violence or threats of violence during the visit. If there is to be a termination of care, there must be a reasonable notice depending on the needs of the patient and other resources available. Notice of termination of care should be in writing and hand-delivered to the patient.

*Caregiver security escort.* There are times when a caregiver must be provided a security escort for a home visit. There are two basic forms that such a security escort can take. One is a uniformed, generally armed security officer in a marked security vehicle.

The escort may transport the caregiver in the security vehicle or meet the caregiver at the patient's address. In the case of the conspicuous security escort, the security officer generally remains outside but ready to respond if summoned by the caregiver. The second approach is to provide a security escort in street clothes or care agency uniform. In this case, the escort usually accompanies the caregiver into the living unit and is introduced as a team member. This type of escort normally involves an unarmed security officer.

*Security education for the caregiver.* It is absolutely essential that all home healthcare staff receive security training and education. This training must reinforce security awareness and practice without frightening the staff. The training should also teach caregivers how to avoid or defuse dangerous situations to include dealing with a threatening dog. Canine strategies often include

- Assessing the dog's reaction
- Showing no fear
- Maintaining eye contact
- Never assuming the dog will not bite
- Not startling the dog
- Calling the dog by name (if known)
- Never attempting to pet the dog
- Having an attack plan, i.e., standing ground, using purse or other bag, backing away slowly

Professional caregivers are very focused on delivering a quality service and do not always assess the environment or perceive danger signs. In addition to formal training presentations, it is recommended that each home healthcare agency develop safety and security policies to be distributed to each caregiver to guide their everyday activities. Information in this regard is identified in [Table 22-1](#).

A good security practice for home healthcare providers is to require them to report to a predetermined member of the office staff upon reaching a specific destination. A supervisor or office staff member in turn is required to implement follow-up procedures in case they do not report in. It is important for a supervisor to know the schedule of the provider, and to be informed of any unscheduled stops. Many agencies provide field staff with cellular telephones to facilitate this process. The emergence of Global Positioning Systems (GPS) to track the movement and location of the caregiver's vehicle has provided another element in providing for the protection and safety of the home healthcare provider.

There will be additional safety practices depending on the agency, such as pre-planned routes, emergency notifications, route deviation procedures, etc.

Home healthcare providers often carry a medical bag but rarely, if ever, narcotics. These bags include equipment, medical supplies, needles, syringes, and common medications. A number of agencies have returned to a more traditional nursing approach and provide their staff with a uniform. Although some home health professionals argue that this practice brings more attention to the provider, many more believe this provides added protection because of the respect and authority given to medical personnel by the public.

**Table 22-1** Security Strategies for Home Healthcare Providers**Home Healthcare Security Strategies**

Take planned routes that are well-traveled streets—not taking shortcuts through unknown areas.

Utilize a reliable, well-maintained vehicle with ample gas supply.

Drive by the client's address for a short distance while assessing the neighborhood (i.e., suspicious vehicles or persons loitering).

Park in the direction of travel you intend to use when departing from the visit.

Park so that your vehicle can be seen from the client's home whenever possible.

Always lock your vehicle and do not leave property exposed in open view.

Setting limits of behavior and knowing when to leave (i.e., presence of guns, knives, or illegal drugs, excessively loud and abusive behavior, physical or sexually aggressive behavior).

When leaving, have keys ready, lock doors immediately upon entering the vehicle, and do not sit in the vehicle checking maps or preparing documentation.

Depart the neighborhood immediately, heading directly to a well-traveled street.

Note any vehicle that pulls out directly behind your vehicle when you depart.

## Patient Treatment Facilities

The vast majority of off-campus patient treatment facilities do not operate on a 24/7 schedule. In fact, some facilities may only treat patients for a limited number of hours per day and some facilities are not open for service every day of the week. There are, of course, exceptions, such as an urgent care/day surgery facility with a limited number of inpatient beds. In this respect, there is a wide variation in needed security safeguards unique to the mission and operating environment of each facility.

It would be difficult to list all the different types of off-campus patient treatment facilities; however, some of the common types are

- General treatment and preventive services, such as general physicals, inoculations, and minor diagnostic procedures;
- Specialty clinics where visiting physicians/treatment technicians schedule follow-up treatment evaluations and services. Examples of these needed medical specialties would include cardiology, ENT, audiology, orthopedics, radiology, pulmonary, dermatology, and neurology;
- Ongoing therapy treatment such as physical, occupational, speech, and orthopedic therapies;
- Day surgery procedures;
- Dentistry.

In addition to facility locations, there are mobile units that provide outpatient treatment and diagnostic procedures on a scheduled basis, as well as blood donor and health education types of community activities.

## Responsibility for Securing Off-Site Facilities (Clinical and Nonclinical)

The responsibility for providing security of patients, property, staff, and visitors at off-campus healthcare organization facilities is the primary responsibility of the senior manager of each facility. In some cases, a senior manager will be on site at the facility on a full-time basis. In others, the senior manager will be responsible for multifacilities and may have other assigned duties and responsibilities. The senior manager should not have full authority (autonomy) in deciding what the protection program for these facilities should or should not be. The planning and implementation of the security program would be a collaboration of efforts by the senior manager and the designated organization security administrator. The collaborative security program would be subject to the security policies and procedures approved by the leadership of the organization. The end result should be that each facility is subject to standard security operating procedures and standardized physical security, equipment, monitoring, and maintenance, with allowances for special needs and circumstances unique to the facility.

## Primary Security Safeguards of the Off-Campus Patient Care Facility

The planning and installation of security safeguards in off-campus facilities is extremely important as many, or most of these facilities, are void of staff for varying periods of time. The integrity of maintaining a locked and secure facility during these vacant time periods is a critical business management responsibility.

## Access Control

Allowing entry, denying entry, and control of the movement of patients within the facility is a basic element of security. All patients should enter the facility at what can be called the public entrance that leads directly to a point of reception. In some cases, the facility will have an ambulance entry point. At the reception point, all persons entering need to state their purpose for being at the facility. The staff person at the reception point, receptionist or triage nurse, would be responsible to facilitate the patient/visitor's controlled visit. A general rule is for an appropriate staff person to be notified that a patient/visitor is waiting. In this mode of operation, the patient/visitor should be escorted from the waiting area, and at the conclusion of their care or business, they should be escorted back to the reception waiting area for exiting the facility. Patients and visitors should not be dismissed from office or treatment areas, which would allow them to roam the facility.

Except in the very small off-campus treatment facility, there should be a specific locked staff entrance electronically controlled by either code or card access. Card access is most common, as the card can be used for identification, access control, and time-recording purposes. During business hours, all ingress doors should be locked, with the exception of the public, staff-controlled entry point. In some higher security-risk environments, it is common to lock the public entry point for certain times, even though the facility is operating in the service mode. An example would be the urgent care facility that

operates from 10 A.M. to 10 P.M. daily. The public entry could be open for free access until a designated time when the door would be locked, say from 6 P.M. to 10 P.M. Locking this door during treatment times would require a system of communication and means to conveniently release the locking mechanism for entry.

## Video Surveillance/Alarms

Each off-campus facility should be protected with the installation of video surveillance equipment on all entry/exit doors and other internal areas. The use of IP-addressable video equipment would permit remote viewing by authorized persons. The video surveillance equipment, when integrated with an alarm system, can provide a high level of security for the closed facility. Door alarms and motion-type alarms can effectively alert a monitoring point of activity occurring.

The use of panic alarms (duress alarms) has limited value in the small off-campus facility. In many cases, the staff does not know the location of these types of alarms, understand their intended use, or know where the signal terminates. When staff members are asked where the signal is sent, over half of the replies are that it goes to the police department, which is rarely, if ever, the case. As discussed earlier in this text, the unintentional experimentation and lack of knowledge of the alarm device generally result in an unacceptable number and use of such alarm activations.

## Security Officer Coverage

There may be a need to schedule security officer coverage for certain off-campus facilities during the times the facility is open or for a portion of the operating time. For example, an urgent care facility that is open from 10 A.M. to 10 P.M. may not require officer coverage during the day, but have a need for such coverage from 6 P.M. to 10 P.M. Another aspect of the off-site officer coverage is that it needs change and can change rather abruptly owing to a change in hours, operating budget restrictions, or outright closure of the facility. These types of changing environments, and often limited hours of coverage, make it extremely difficult and somewhat inefficient to staff as part of the main facility in-house security officer staffing schedule. The use of a contract security service may be a good alternative staffing choice. The contract staffing model provides a fixed cost for budgeting purposes, a relatively easy change if a certain officer does not fit in with the requirements of service or if there is a change or elimination of hours of needed service. In general, there are fewer officer-training requirements involved and career ladder concept is not an issue. Client interpersonal relationships with patients and visitors are key elements of this type of security officer service.

## Vehicle Security Patrols

With the advent of security technology, the value of periodic security officer vehicle patrols is a greatly diminished security practice during the time period the facility is closed. The use of such patrols during operational hours, however, can be productive in

terms of a periodic security officer presence. In order for such patrols to be cost-effective, the facilities to be patrolled need to be in relatively close proximity to each other. A general rule of thumb is that vehicle-driving time should be less than 50% of the combined time actually spent on the premises of the facilities.

A relatively new innovation is the virtual patrol of off-campus premises via an integrated video surveillance system. In this approach, virtual patrol tours can be made that allow for a system security officer or dispatcher, or outsourced provider, to monitor the environment and the security of the building via strategically located cameras. This approach often incorporates random patrol tours throughout the day and night and on-demand observation if an alarm is received.

## Security Signage

The same type of security signage used at hospitals and medical centers should also be used in the off-campus locations. The use of security signage was discussed in *Chapter 17, Physical Security Safeguards*. In addition, a very important emergency information sign, visible from outside the facility, should be in place at all facilities that do not operate on a 24/7 basis. The emergency information sign is primarily directed to, but not limited to, public safety agencies. The sign should contain information that allows the public safety agency, or other persons, to quickly notify the proper person of the healthcare organization of an emergency situation that may exist. One might immediately think of fire; however, vehicles running into the building, severe weather damage, or a breaking and entering are examples of other situations that might occur. These unexpected types of incidents may require the deployment of security personnel to temporarily secure the facility, obtain the services of a “board-up” company or the need to make immediate utility-type repairs.

## Night Lighting

The issue of providing adequate night lighting in the parking lots and at the exterior (walkways) of the off-campus patient care facility is extremely important and can often be problematic. The night lighting levels of 16 freestanding outpatient care facilities were conducted as part of an overall security risk analysis project. All of the facilities were open until 9 P.M. or later. The results were that six facilities had adequate lighting, four facilities had marginal lighting, and six facilities had inadequate lighting for security and safety levels of light. In reviewing the results of the lighting survey, it appeared that the majority of the buildings had been built by developers. The buildings were basically designed as complexes to be leased by day-business entities. In all 16 facilities, the night lighting was adequate for the closed, locked, and alarmed building. The night lighting is just one issue, but is a good example of why security and safety professionals should work closely with organization property managers during the lease or during new building design and layout.

When the organization builds an off-campus patient care facility, the night lighting issue is generally resolved in the planning and design process. The issue often becomes



problematic when the organization contemplates leasing space in an existing building. The healthcare organization and the building owner will work together to complete the details of the interior build-out or space-design changes. The issue of inadequate night lighting does not generally surface until the onset of delivering patient care services or there is an occurrence of a security or safety incident. At this point, the owner is generally reluctant to spend extra money for night lighting, since he already has a lease agreement in hand. In some cases, the healthcare organization will fund the cost of such lighting, but they are, of course, reluctant to invest money in capital improvements to a facility they do not own. If lighting can be increased to an adequate level with lighting fixtures mounted on the building, it is more achievable than a project that requires burying additional electrical lines with the addition of anchoring light fixture standards in asphalt- or cement-surfaced parking lot.

### Organizing the Off-campus Protection Program

There are at least three major challenges in organizing and implementing off-campus facility security programs. These challenges are the logistics of supplies, transportation, and services support of the healthcare organization's main campus; the inherent culture of off-campus management, which often says "we have our own unique needs and we will operate more semiautonomously than if we were part of the main campus;" and of course the funding of security program elements that may or may not have been adequately addressed in the planning stages. The parent organization will usually judge the success of a new start-up operation by its financial performance almost from day one. Since security is considered overhead and nonrevenue-producing, off-campus administrators are quite reluctant to increase security overhead expenses.

#### *Security Program Administrative Structure*

The structure and general operating authority of the off-campus facility security program should reside as a component of the parent healthcare organization administrative plan. This does not mean that the administrator of the off-campus patient care facility will not have any authority in day-to-day operations. It simply means that the collaborative authority of the facility administrator and the director of corporate security should be thoroughly understood and stated in an approved authority matrix.

The majority of healthcare provider organizations today have either a few or many off-campus clinical and nonclinical facilities. The size, number, geographical locations, types of patient care, types of nonpatient care services, and neighborhood profiles make each of these systems unique unto themselves. It provides the opportunity for the Director of Security to develop an efficient and effective organizational model to accomplish the level of protection that fits the circumstances. [Figure 22-1](#) is an example of an organizational model that security directors can adopt, modify, or reject according to their needs and requirements. The important point is that there needs to be an organization chart that puts the organizational structure into perspective.

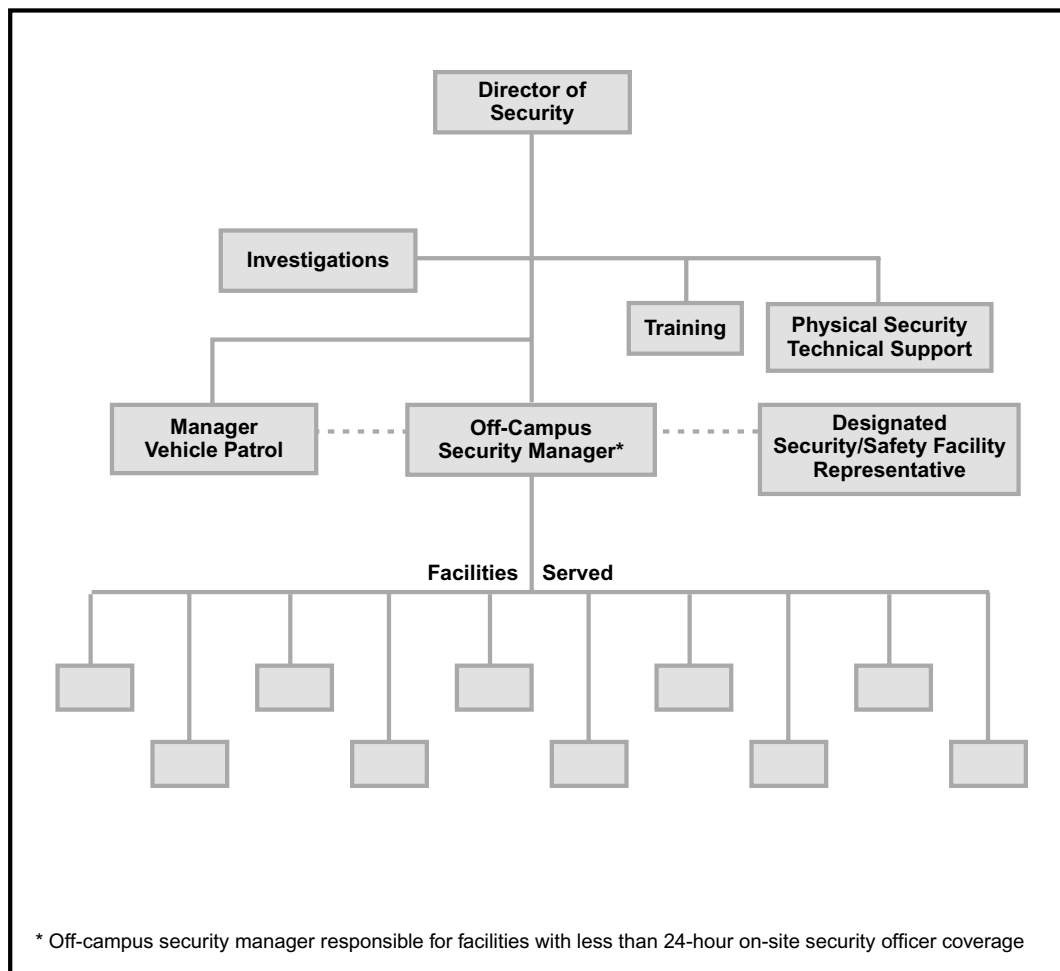


FIGURE 22-1 Security operations/organization model for servicing off-campus clinical and nonclinical facilities.

### *Security and Safety Representative*

The concept of having an appointed Security and Safety Representative for each off-campus facility enhances the communications link between the facility and the corporate security program. The representative is a staff person assigned as a full-time working staff person at the facility. The responsibility for security and safety duties is simply written into the person's position description. The representative is not necessarily trained in the field of security and safety but administratively coordinates these activities for the specific facility. Examples of this coordination include

- Requesting new keys, issuing keys, retrieving keys, and accessing identification badges
- Reporting malfunctioning security equipment to central security

- Preparing security incident reports in absence of security officer coverage and forwarding those reports
- Requesting investigative activity
- Communicating staff security concerns and recommendations upward through the chain of command
- Requesting specialized security support for temporary situations

The representative performs similar activities and duties in regard to safety issues and concerns.

There is a formal training class and general meeting required of all security and safety representatives on a bimonthly basis. In addition, a corporate security staff person, a safety staff person, and the facility representative should complete a periodic on-site inspectional/review tour of the facility on a quarterly basis or more often as the facility profile dictates. During these rounds, a special point is made to inquire and engage staff relative to any security or safety issues that they may wish to discuss.

#### *Security and Safety Incident Report*

The security and safety incident report is a basic element of the off-campus security system. These reports provide a profile of the safety and security environment. The reports are generally electronically forwarded to the manager of off-campus security. The manager reviews the report, which may be filed for future use as required, decides to look into the matter personally, or requests corporate investigation or physical security support as appropriate. A spreadsheet database is maintained that allows for the preparation of a consolidated report comparing security incidents of each facility. In this type of system, the Materials Management Department is prohibited from replacing any equipment lost or stolen without a completed security incident report, which must accompany the “Request to Purchase” form. In this same vein, no off-campus facility is allowed to add new security equipment or replace equipment unless approved by the manager of off-campus security.

#### *Cash/Payment Handling*

Virtually all off-campus patient treatment facilities collect payment for goods and services rendered. Some nonclinical departments also collect money or may have substantial petty cash funds. Most facilities that have been operating for any length of time will not be able to boast that they have never encountered cash/receipt losses, including fraud. Money just seems to attract safekeeping and accountability problems. There are several money-handling security principles that apply to the off-campus facility. A daily courier service is essential to the successful off-campus operation to provide for the movement of various supplies, reports, and equipment, including cash and other financial instruments. The courier schedule should be such that a pickup is made late in the day, to minimize the amount of money, checks, and charge card receipts kept in the facility overnight. In the small facility, the courier service may be every other day and the larger facility may even require the services of an armored car.

In the typical system of money transfers between the cash management office at the main facility and off-campus locations, a locked moneybag is used. In this system, the courier picks up a locked bag and subsequently delivers a locked bag. Since some deliveries of the moneybag to the main facility will occur after the cash management office is closed, there is usually a drop safe arrangement to store and protect the bag. *Chapter 21, Areas of Special Concern*, discusses security of the cash management office in further detail.

There will always be the need to store cash, checks, receipts, and possibly valuables during nights and weekends at most off-campus patient care facilities. Each facility should have a small, yet substantial, drop safe for this purpose. The safe should be securely fastened to the floor or concrete sidewall.

### Nonclinical Off-Campus Facilities

The list of nonclinical departments or functions of healthcare organizations that are often located off the main campus is exhaustive and is usually driven by space needs of the main facility. Common off-campus nonclinical facilities include materials management storage, staff training classrooms, marketing, planning, accounting, legal, and record storage, to name a few. The security safeguards for these functions should be facility management, with consultation and support of the main facility security director. The security risks and safeguards to be implemented may be much more diverse than those facilities providing patient care.

### References

1. Lohr, K. Abortion providers on high alert. (2009, June 3). *NPR*. Retrieved from <http://www.npr.org/templates/story/story.php?storyId=104841479>.
2. Home healthcare opens door to abuses. (1996, November 11). *USA Today*, 11B.
3. Home healthcare opens door to abuses. (1996, November 11). *USA Today*, 13B.
4. Tribute to a home care nurse. (1996, December). *Colorado Nurse*, 10.
5. Milburn, J. (2000, February 8). Three fatally shot in Girard. *Topeka Capitol-Journal*. Retrieved from [http://www.cjonline.com/stories/020800/kan\\_girard.shtml](http://www.cjonline.com/stories/020800/kan_girard.shtml).

## Parking Control and Security

Medical center parking areas, whether surface lots or multilevel structures, are often scary and downright dangerous places. The random shooting death of a police officer in Wilmington, NC, as he and his wife were leaving the hospital at the close of visiting hours; the critically injured woman in Omaha, NB, who was shot in a medical center parking lot by an assailant who was attempting to steal her purse; the hospital parking attendant in Philadelphia, PA, who was shot to death during an armed robbery; the healthcare office worker in Indianapolis, IN, who was locked in the trunk of her vehicle while the assailant drove her vehicle out of the parking structure are examples of tragic incidents occurring with great frequency.

The demand for medical center parking has increased drastically in recent years. The demand for more parking spaces has been driven to a large extent by the trend to expand outpatient services. The patient-to-bed census parking demand ratios are thus outdated for planning purposes. In addition, many benchmarks and tools previously utilized to project medical center parking needs have become marginally useful and basically obsolete. Even though parking needs and parking issues have always been a major concern for healthcare organizations, they frequently fail to receive proper planning processes, including providing necessary security safeguards. A recent parking survey conducted by a Colorado hospital revealed that every 100+ -bed hospital in the state believed they had an inefficient number of parking spaces to meet their needs.

Each healthcare organization has its own identity in terms of product mix (types of services), market share, patient/visitor/staff composition, and degree of public transportation, which are all basic factors in determining parking space needs. The control of parking is a major activity for medical care facilities. This responsibility is sometimes considered to be within the purview of the security function and at other times is assigned elsewhere in the organization. The context of parking control does not always include the necessary elements of protection. Some argue that parking control is not a true function of security and that it is a separate area of facility services. All “parkers” want to park as close as possible to their intended destination. As facilities grow and change, the demands for parking change. It is not necessarily the number of parkers but convenience that makes control difficult. Many healthcare organizations periodically undergo major relocations of entrances and services. Such changes often create a new front door, and parking needs change as a result. In designing parking accommodations, the following is a basic general priority listing:

- Handicap parking (required by law)
- Emergency services (patients/transporters)
- Ambulatory patients with impaired mobility
- Outpatients
- Clinic patients
- Delivery drivers
- Visitors
- Staff (including physicians, volunteers, and physician office staff)
- Vendors and educational program attendees

Despite the rather low parking priority for medical center staff, they account for 60–70% of the parking needs.<sup>1</sup> The protection of people and property on medical center property, including parking areas, is a major security responsibility. This protection responsibility includes preventive patrols, escorts, response to calls for services, investigation of security-related incidents, and physical security monitoring. The parking accommodations of different healthcare facilities present unique control and protection situations. One constant factor is that there are never enough parking spaces. The shortage of spaces is most acute during the day on weekdays, when employee staff is at its high point and clinics and outpatient services are in full operation. The most acute shortage is when day-shift employees are still at work and the arriving second shift must find parking spaces. Once the day shift leaves, there are generally an adequate number of parking spaces available.

Since the security department is generally responsible for enforcing parking regulations, it receives the brunt of employee, visitor, and patient dissatisfaction with the real or perceived lack of parking facilities. Unfortunately, this dissatisfaction with parking has a direct negative effect on the image of security and the entire organization. In addition to enforcing parking regulations to affect orderly use, the security effort is concerned with the ever-growing number of assaults, thefts, and incidents of vandalism that occurs in parking areas. Numerous major lawsuits against medical centers allege inadequate parking area security. Litigation can result in punitive as well as general damage awards. In Pittsburgh, PA, the security in parking structures became such an issue that the city enacted an ordinance mandating certain security provisions. The law covers any structure that charges guests, employees, or the public to use a parking space. The law enforced since 1985 by the Bureau of Building Inspection requires the following:

- A uniformed security guard must patrol all levels of the structure once every 30 minutes, unless detained for security reasons.
- Patrols must be verified by activating a recording device on each level.
- Emergency communication devices must be installed on each level.
- Lighting must project a minimum of 5-foot candles in all areas.
- Emergency phones must be installed in elevators.
- Directional arrows must be painted on walls to indicate exits and elevators.

Since the implementation of this parking structure ordinance, the complaints from users have been reduced and the wave of assaults on parkers has been virtually eliminated.

Perhaps one of the strictest parking garage security laws in the country is in effect in Minneapolis, MN. The law's requirements for security became effective in 1990 and have proven to be very effective in terms of public safety.<sup>2</sup>

## Types of Parking Areas

Parking areas can generally be categorized as street parking, surface (at grade) lots, free-standing structures, and structures that are physically connected to healthcare facilities, plus numerous delivery and emergency vehicle short-term parking spaces. Although the application of security safeguards will vary depending on the type of parking, the objectives are the same:

- Establish a user-friendly feeling
- A high level of safety in both perception and reality
- Property protection
- Expedite the patient care mission of the organization

### Street Parking

Parking on side streets around the medical care facilities presents a security challenge. This parking is on public streets and is generally outside the realm of the organization's protection responsibility. In a practical sense, however, persons who are assaulted and vehicles that are broken into on these side streets negatively affect the healthcare organization. It is not uncommon for security to escort employees or visitors to their vehicles, which are parked off facility property. Security escorts should, however, be restricted to a maximum of one block, and this restriction should be strongly upheld by the organization. When security officers are more than one block from the property, they are not providing a visibility at and around the facility, surveillance, or maximum response capability. This extended escort service may help one person to the detriment of others.

Street parking can cause community relations problems in addition to protection problems. Neighboring homeowners generally resent cars parked along their streets all day because they restrict homeowner use and bring a certain amount of congestion and litter. The homeowner generally faults the healthcare organization for the situation, since the organization is more defensible than just vehicles and people. Many communities surrounding the medical campuses have implemented permit parking or 2-hour parking limits, enforced by the local police department, to minimize street parking by employees and visitors to the facility.

### Surface Parking Lots

Surface parking lots are slowly disappearing from large city and urban medical centers. The cost of land and the fact that many facilities are landlocked generally results in the construction of parking structures when parking areas must be expanded or replaced. Security for surface lots generally consists of access control, emergency communication

devices, fencing, lighting, security patrols, and observation posts. Enclosed observation posts, somewhat elevated, in the parking area offer several advantages. Not only do they provide shelter for security officers, but they also present a visible security safeguard. Video surveillance is not widely used for surface lots because of its low cost/benefit ratio and limited span of view. When video surveillance is needed, pan-tilt-zoom cameras are most often used. Programmed on a digital patrol path, the cameras can be used to provide surveillance of the entire parking lot. The central monitoring station can also control the camera view during events that may occur in the parking lot. Of specific importance in surface lots is that landscaping be well placed, and properly maintained, to eliminate hiding areas, reduced visibility, and reduced lighting levels.

## Parking Structures

As land values increase and the available land around healthcare organizations decreases, parking structures become a cost-effective alternative to surface lots. Modern structures can be designed to achieve the user-friendly atmosphere and produce a general feeling of security and safety. Among the desired design features are raised ceilings, extensive use of glazing materials, proper lighting, bright colors, legible signs, and the basic elements of physical security.

Parking structures provide concentrated parking, but at the same time they create certain security risks. Many such risks can be eliminated or minimized through proper security design, which should begin with the first architectural drawing. Architectural firms without security design experience should advise their clients and take steps to obtain security advice. The basic security considerations for parking structures include the following basic security safeguards:

- The structure should provide the maximum span of vision on the parking levels and should mitigate the negative aspects of interior support columns and dark corners.
- Lighting should comply with the standards of the Illuminating Engineering Society of North America (IESNA). This standard includes a 3–5-foot candle lighting minimum throughout the structure. Entrances should have 10-foot candles of lighting to make it a standout and increase visibility.<sup>3</sup> It is suggested that metal-halide or white-light sources be used, which provide reliable color recognition, increase the ability of witnesses to identify attackers, and improve the clarity of visual imaging. The installation of lighting should take into consideration the failure rate of the various components of the system. At any given time, approximately 18–22% of the lighting system may be inoperative. Thus, the lighting standards should be exceeded by approximately 25% so that minimum lighting levels are maintained. A common method to counteract the effect of burned-out lamps is to use several lamps in one luminary. In high-risk malicious destruction environments, it may be necessary to incorporate polycarbonate lenses to protect the luminaries. The interior of the structure should contain some light-colored surfaces (e.g., supporting columns and walkway areas). Light-colored paint increases the



effectiveness of lighting and conveys a feeling of security. An important aspect of parking structure lighting is that of uniformity. Drivers should not experience passing from light to dark areas. There should be lighting in the parking stall and not just in the driving aisles. Another important lighting consideration is to reduce glare. Glare is a potential hazard for all drivers, but is particularly dangerous for senior citizens and others with impaired vision.

- Parking areas should be well maintained and clean. Many healthcare organizations will schedule periodic cleaning throughout the year to wash walls, clean off the dust and grime that collect on light fixtures, as well as add a new coat of paint to the walls and ceilings.
- Stairwells and elevators should be enclosed with appropriate glazing materials, to protect patrons from wind or inclement weather or an open design in moderate climates. [Figure 23-1](#) demonstrates a parking structure with an external glass stairwell.
- Stairwells, walkouts, and traffic ingress/egress points should, whenever possible, open onto the facility's property, not the street.
- Elevators should be located near the main entrance so that patrons are highly visible to the public.
- Emergency ground-level stairwell exit doors should be alarmed as part of the access control system.
- Emergency telephones, or call stations, should be connected directly to the central security station or the facility's telephone operator. These devices are generally hardwired as part of the parking lot or structure construction with minimal cost. If such devices are to be installed in existing facilities, the feasibility and cost-effectiveness of wireless systems should be explored. Call stations must be



**FIGURE 23-1** Picture of a parking structure with external glass stairwell.

conspicuously marked in two different ways. First, they should be marked to be identifiable for their intended purpose and be able to be seen from great distances. A blue light is commonly mounted above the call station on both hospital and college campuses. Conspicuous signage is also recommended to inform parkers and point to emergency call stations. Second, the station should be prominently marked with a location, so that callers can accurately describe their location to the dispatcher. Even though many such communication devices automatically show the caller's location at the answering point, it is still desirable to indicate the user's location on the device at the calling point. There are some systems that activate a strobe light when the communications device is activated. This activation is intended to scare away potential troublesome persons and to visually indicate a clear destination path for responding security personnel. Many newer systems have also incorporated a video image capability, allowing the dispatcher to visually see the caller.

- Openings on the ground floor, large enough to allow people to climb through or to pass large objects through, should be eliminated. Decorative wire mesh or other barriers can be installed that meet the security objective, yet provide light and visibility.
- All entrances/exits should be capable of being closed (locked off) during low traffic periods or emergencies, including gates that prohibit pedestrians and vehicles from entering the structure. [Figure 23-2](#) is a concept drawing of primary parking structure entrances/exits being internal to the hospital grounds with limited use of exiting onto the street at high traffic-volume times.
- Emergency release devices should be installed on stairwell emergency exit doors.
- Frequent security patrols should be scheduled. The frequency will depend on the time of day, local crime rate, number of reported incidents, location, and other security safeguards that have been installed within the structure.
- Cashier booths should be placed outside the structure so that cashiers have a better view of loiterers, stairwells, and general traffic.
- Covert parking area surveillance posts should be provided. Ideally, there will be one or two such posts on each level, allowing security to view any part of the structure. One-way glazed observation posts are generally used. All enclosed areas, such as equipment spaces and storage areas, provide an opportunity for observation posts with little additional cost. By simply including a small window, this added element of security can be achieved.
- Cost overruns in construction seem to be a standard. When cost overruns occur, security is generally the target of cost cutting. Even when planned security applications are eliminated, the proper design of the structure can accommodate later retrofitting at a more favorable cost.

### *Video Surveillance*

Many questions arise concerning the use of video imaging for parking security. The first question is whether a video surveillance system is needed. Sometimes it is decided that an area should be monitored before a clear need has been established. The use of video

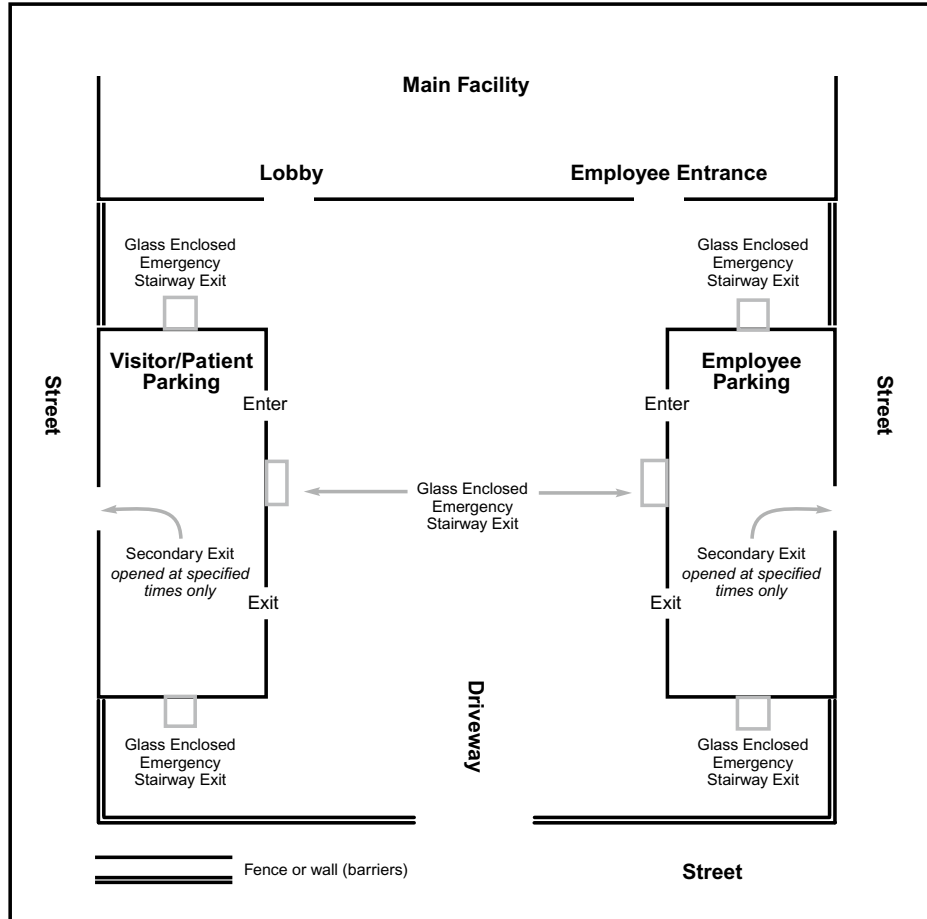


FIGURE 23-2 Example of the CPTED security principle of territorial reinforcement and clear lines of sight.

surveillance is somewhat prevalent in parking structures, yet many of these structures have various elements of design that do not lend themselves to this physical element of security. If used, an important first step is to determine the philosophy of use for the video surveillance system. A common philosophy is to design the system to monitor all entrances and exits and strategically locate cameras at elevator lobbies, stairwell exits, and other high pedestrian-traffic areas. Rarely is it a cost-effective use of resources to place cameras throughout the entire parking garage, on all floors, attempting to monitor all areas. With varying sizes of vehicles, many camera views are frequently blocked. If cameras are placed in the middle of the traffic lane, the camera view is typically limited only to viewing vehicular traffic in the parking garage, which has limited security value.

All video surveillance systems require effective monitoring, regardless of the size of the system, and this is extremely difficult to achieve. Even when effective monitoring is in

place, the reaction to monitored incidents is of equal importance. The response of security, police, or fire personnel must be quick and properly directed.

Opponents of video surveillance in parking garages point out that it does not give directions, it does not generate people-to-people public relations, and it does not respond to incidents. The live video monitoring or recording of an incident does little good without a quick response capability. The argument that video surveillance may help solve a crime is valid; however, a primary objective of the system is to contribute to the prevention of incidents. The cost of a video surveillance system does not end with its purchase and installation. Systems require monitoring, maintenance, and ongoing replacement expenditures. From a liability standpoint, malfunctioning equipment must be repaired immediately or alternative security safeguards must be implemented until the system is up and functioning as designed.

### *Signage*

Signage and graphics in parking areas serve several purposes, including control of parking, the providing of general information (directions), and security information. Information signage that orients parkers and enables them to move quickly in and out of the parking area makes them less vulnerable to a security-related situation. Security signage indicating video surveillance of the area and the emergency call stations information signs will generally provide a greater feeling of safety. This security signage also serves as a crime deterrent.

Organizations may want to include signage that tells parkers to lock their vehicles and/or not to leave valuables in their vehicle. A sequel to the “locking” sign is notice to the parker that the organization is not responsible for lost, stolen, or damaged property. This type of signage is recommended, but may present a somewhat defensive attitude, and thus not have administrative support. Even without the locking/disclaimer signs, organizations should have a strong administrative policy that prohibits reimbursements, except in special circumstances.

### *Personal Communication Devices*

There are emergency communication devices that can be carried by staff that utilize a radio frequency (RF) to alert a monitoring station of an emergency situation. The employee can summon help by simply pressing a button. An activated device, sometimes referred to as a pendant, will report to a transponder pedestal located within the general area and relay that location to the monitoring station. The cost of these systems is quite high and there is always the shifting of parking areas, the lost or forgotten device, and malfunctions that can result in a failure to provide the anticipated and intended response.

## Parking Shuttle Service

Some facilities that have been unable to increase campus-parking capabilities have instituted shuttle services to off-site parking facilities. This type of parking arrangement is generally directed to the employee so that additional on-campus parking can be available to

patients and visitors. Suitable parking areas are sometimes available near the facility, but are not within walking distance or pose too much risk for the exposure to a potential street crime to be an acceptable option. Shuttle buses have proved effective for transporting employees to and from the work facilities. In the typical shuttle system, security department employees drive a passenger van or bus at frequent intervals between the parking lot and the facility during the early morning and late afternoon hours. The frequency of such service is reduced during the day. When an employee needs to leave during the middle of a shift or is held over past the closing time of the lot, security is contacted and often a special trip is made for that employee, depending on the circumstances. This special shuttle trip is then utilized to provide a random security patrol of the parking area. Likewise, there must be arrangements made to accommodate random arriving staff. Organizations have tried many incentives to entice employees to use off-site parking areas, including:

- Comfortable waiting areas (heated and air-conditioned as appropriate)
- Complimentary coffee, rolls, and morning papers
- Coupons for free or reduced cost for food in the facility cafeteria
- Weekly prize drawings
- Car washes while the vehicle is parked for the day for a reasonable fee
- Attended parking lots

The main complaint of the use of a shuttle service is transportation waiting time. Thus, organizations must ensure that they have sufficient resources before embarking on a shuttle program.

One Midwest hospital asked employees to park in a church lot six blocks from the hospital and to walk to and from work. Instead of putting money into shuttle service resources and incentives, they paid employees to park in the off-site area. The program was oversubscribed by employees, and there was a continual waiting list for vacancies.

## Valet Service

The use of valet parking for healthcare patrons is not new, but it is growing. The shortage of convenient parking is the greatest stimulus to the valet parking system, but proponents also cite the marketing advantage of this program. Some organizations charge for valet parking, others offer the service free. Organizations that undertake a valet parking program should provide adequate supervision, and they should review their insurance coverage regarding this type of operation. The hours of operation should be clearly stated and the procedure for retrieving vehicles after hours should be established. Security often becomes involved in the after-hours retrieval of vehicles.

## Types of Parkers

Those who use facility-provided parking can be divided into several distinct categories, including day-shift employees, afternoon-shift employees, night-shift employees,

outpatients, inpatients, physicians, visitors, and vendors or outside service representatives. Despite flexible scheduling and the use of 10- and 12-hour shifts by various hospital departments, there is still a discernable day-, afternoon-, and night-shift demand for parking. The most common approach is to assign each category of parker to a specific parking area. During the day, the nearest parking is generally assigned to outpatients, physicians, service representatives, and visitors, owing to their short-term use of parking space. Whether appropriate or not, physicians usually demand and receive special attention when it comes to parking.

### Afternoon-Shift Employees

The afternoon-shift employees are the ones who are most affected by the inadequacy of parking space because the day shift is still on duty when they arrive. A common solution is to designate a special “3–11” lot (named for the hours of the typical afternoon shift), which is opened approximately an hour before the afternoon shift reports for work. Entry to this lot is generally controlled by a security officer unless automatic controls are installed. This lot, which is vacant during the morning hours, can also be used to accommodate people attending morning meetings and appointments, but must be tightly controlled to assure that these temporary parkers have cleared the lot by the required time.

If the 3–11 lot is not adequate to accommodate all afternoon personnel, the organization should consider placing designated employees in the physician’s parking lot. In most facilities, the peak time for physicians is in the morning, before they go to their offices. Of course, not all open spaces should be used by second-shift employees, because some physicians stop by the facility after their office hours. It should be noted that the relatively new concept of the “hospitalist” position at most hospitals has reduced the number, frequency, and need for private physicians to make regularly scheduled hospital rounds.

The fact that afternoon-shift personnel may return to their cars late at night presents special security vulnerabilities. For safety reasons, it is desirable that shift employees park together. Maximum security officer coverage in the parking lots is advisable during late night and early morning shift changes.

### Late Night–Shift Employees

Late night–shift employees generally have many places to park and, when left to select their own options, may create a fragmented parking configuration. Facilities that staff two shifts per day (usually 7 A.M.–7 P.M. and 7 P.M.–7 A.M.) can create some shortage of staff parking, again due to oncoming shift staff arriving before the offgoing shift vacates their spaces. There should be a designated area for these employees, which is typically as close as possible to the designated facility night entrance(s). By concentrating these employees and their vehicles into a specific area, a maximum amount of protection for both employees and vehicles can be provided.

## Automated Controls

An electronic, card-activated gate is considered to be cost-effective for parking areas with as few as 20 spaces. The use of RF technology provides a hands-free control system with card reads of 10–14 feet. Automatic gates with a minicomputer offer many control features, including the ability to set time parameters for card use, to invalidate a card at the output unit, and to provide data on the attempted use of invalidated cards. In addition, some systems render cards invalid once they have been used to enter the parking area until they are used to exit. This feature, known as *anti-passback*, prevents one card from being used by several people. Card-activated gates are predominantly used at the entry and exit points of parking areas. The card-activated device can also be used within the parking area itself to reserve and control an area for valet parking, afternoon staff, or physicians. In addition, the parking card can be used to provide entry to locked physician and staff facility entrances.

## Traffic Flow and Space Allocation

In determining traffic flow and space allocation, the trend toward small vehicles is both an advantage and a disadvantage. When most vehicles were the same size, parking spaces could also be uniform. This limited the number of available spaces, but it made space allocation a rather simple matter. Today, the size of the space needed for small vehicles and the width of the traffic aisles can be reduced. The problem is to determine how many spaces of each size are required at a given time for a particular parking lot or whether certain areas should be designated for all large cars and trucks or all small cars. Not only are one-way traffic lanes with angled parking expedient, but they are also safer than straight, or 90°, parking. The difficulty of parking in a space angled at 90° and the excessive size of the traffic lanes required can make this type of design unsatisfactory. During periods of low demand, it is recommended that certain parking lots, sections of lots, or parking structure floors be closed off. This improves the safety of people walking to or from their vehicles. Naturally, the closed areas should be those that are the greatest distance from the facility entry/exit point. The more concentrated the parking, the greater the number of people going to and from vehicles, which to some extent deters assaults, vandalism, and break-ins. In addition, by closing lots or sections, the security patrol area is reduced, allowing a more concentrated preventive patrol in the occupied parking areas.

## Pay-for-Parking

Recent trends have favored pay-for-parking at medical care facilities. Facilities that have charged visitors for some time have recently decided to charge everyone who parks in their lots. Visitors are generally the first to be charged parking fees and physicians are generally the last. When the pay-for-parking program is the responsibility of the security

department, security can be transformed from an overhead cost to an income-producing department. Some healthcare organizations completely fund their security operation from parking revenues. The outpatient and visitor parking areas produce the most revenue because of their high turnover. The method of collecting parking fees should be closely examined. For employee parking, a monthly fee can be deducted from the payroll checks at relatively little administrative cost. The visitor lots can be controlled by automatic equipment, which has a high initial cost but may prove economical over a short period of time.

The decision to use personnel to collect parking fees should be carefully evaluated as theft of funds by the cashier appears to be the rule rather than the exception. In addition, providing for accounting controls and backup personnel in case of absences can prove much more costly than automatic equipment. The parking attendant cashier does, however, provide an element of safety for both people and property. The presence of an attendant is also a public relations resource, assisting parkers with directions and other courtesy assistance. When collecting parking fees at the point of service (in the lot or structure), there is always the risk of a robbery. In this respect, attendants should be protected by appropriate glazing, a communications device, proper lighting, security patrols, and regularly scheduled and frequent pickup of cash receipts. When automatic equipment is used, stringent controls should be established regarding the collection of money from the machines, and these controls should be audited frequently.

## Parking System Violators

Parking violators present a series of control problems. Fire lanes must be designated and patrolled to ensure that vehicles do not block the lanes, lots must be checked to ensure compliance with the parking plan, and short-term parking areas (such as delivery parking and parking just outside of the Emergency Department) must be constantly monitored. Most security departments issue parking violation or safe parking reminder notices to help control nonconforming parking. In most cases, these violation notices have only a minimal effect on regulating parking. Only when hospital administration takes a strong support role will the violation notice be highly productive. See *Chapter 5, Managing the Basic Elements of Healthcare Security*, and [Figure 23-3](#), for an example of a parking notice.

Various other methods of increasing severity may be necessary to correct parking abuses. These methods include city parking tickets, immobilization devices, and the towing of vehicles. The immobilization device, sometimes known as the Denver boot, a wheel immobilization device, has proved effective in many programs. As noted in [Figure 23-3](#), the boot forces the violator to report as directed, and thus the organization can exert a high degree of control. Vehicle towing is always the last resort but is an effective mechanism to gain compliance. There is, however, an abundance of vehicle towing episodes that have gone wrong in one way or another.





**FIGURE 23-3** The Denver boot wheel immobilization device.

Warning letters and follow-up by department supervisors are common procedures for dealing with employee violators. In one system, the first violation earns the employee a warning notice and subsequent violations result in successively higher fines, which are collected through automatic payroll deductions. This system works; however, again, strong administrative support is required to implement and manage this type of parking patrol program.

## Technology and Parking Control

The use of computer technology is becoming commonplace in the administration of parking control systems. Software programs are readily available that permit tracking of parking violations and efficient issuing and control of parking permits. Once the database of information is established, the various programs allow a multitude of search capabilities. In addition to helping manage the day-to-day program, the computer allows the periodic production of activity and planning reports.

## References

1. Catherine, Q. (1996). Space odyssey. *Health Facilities Management* (June), 30.
2. Travis, J. Crime prevention through environmental design in parking facilities, *National Institute of Justice*, Research in Brief, April 1996.
3. Randall, A. (2008). CPTED for parking lots and garages. *Security Technology & Design*, (October), 42–46.

# Emergency Preparedness—Planning and Management

The planning and management of emergency incidents and conditions that healthcare organizations face daily come in many sizes, shapes, and colors. While some of these situations are intentionally created by man, others result from unintentional accidents, and still others are weather related. Each and every day, facilities react to a variety of emergency conditions.

Emergencies can be divided into internal and external situations for the purpose of this text. Regardless of the nature of the emergency, the organizational response will be quite different when the emergency condition exists within the facility from when it occurs at some distant location. The actual emergency response programs of healthcare facilities indicate that much more effort has gone into a prepared response to external emergencies than to internal emergencies. Exceptions can be found in the areas of fire safety and bomb threat programs, in which various regulatory and accrediting agencies have considerable involvement. A general list of situations that require emergency planning is difficult to compile; however, the situations listed in [Table 24-1](#) should serve as a starting point, depending on the geographical location and type of patient care facility. The media and healthcare management publications have reported case histories for all of these listed emergency situations.

## Basics of Emergency Planning

Patient care facilities should perform a hazard vulnerability analysis (HVA) to identify potential emergency events that have the potential to impact the ability to meet a demand for services. In reviewing the list of potential emergencies, security practitioners should divide these situations into two categories: those that are most likely to occur and those in which the security protection system will be involved most extensively. Security activity at the facility will be fairly standard if the emergency occurs away from the facility (external); that is, involvement will be in the general areas of access control (people and vehicles), information dissemination, and the procurement of supplies and equipment. The security response will primarily be a support role in the care and treatment of patients. A different involvement is indicated when the emergency situation occurs within (internal) or in the immediate area of the healthcare facility. As a general rule, the plan for security response to any emergency should be based, as a foundation, on everyday security safeguards and organizational resources in place. In other words, handling emergency protection

**Table 24-1** Situations Requiring Emergency Planning

<b>Man Made</b>	<b>Accidental</b>	<b>Natural</b>
Bombs/Arson	Fires	Earthquakes
Strikes/Pickets	Hazardous Materials	Hurricanes
Terrorism	Construction	Snowstorms
Gangs/Mobs	Utilities Failures	Tornadoes
Civil Disturbances	Transportation Incidents	Floods
Pandemics		
Active shooter		

needs should be viewed as an extension or expansion of the regular day-to-day security program. When facilities develop complex emergency plans that greatly differ from the normal handling of patients and basic pathways, confusion and inefficiency may result when the plan is activated. It is understood that circumstances may, however, dictate such changes. A case in point is the casualty triage receiving area. If this activity is moved from the normal triage location to another location, supplies and equipment must be moved, and police officers, firefighters, ambulance drivers, and facility personnel must be reoriented to respond to a new and perhaps unfamiliar location. The protection management plan then also becomes more complex and often unnecessarily burdensome.

### Federal Government, The Joint Commission, and International Association for Healthcare Security and Safety

The whole issue of healthcare emergency management took on a new look and new emphasis as a result of the September 11, 2001 terrorist attack. The major change and impact of this event was to significantly interject federal and state government into emergency planning and response for everybody, including healthcare. Following the massive federal initiative, The Joint Commission (TJC) made changes in their approach to emergency management. In 2009, TJC created a new, independent section for addressing the emergency management accreditation requirements. This subject had formerly been a part of the section on the Environment of Care.

The two main areas of healthcare emergency management receiving significant and increased attention are: serving the medical needs that involve a medical surge capacity and the sustainability of the healthcare organization to function in their role with little or no outside support (i.e., utilities, supplies, food, etc.). In addition, it has become mandated that healthcare provider organization emergency planning must include other community and regional entities in an integrated and coordinated effort.

The term emergency, as used in context of the healthcare provider organization, can be any event that disrupts patient care services. Some emergencies are temporary

and somewhat unremarkable relative to their impact on the organization, and others can be of a permanent and disastrous event that can completely shut down the facility. A strong wind may cause property damage, with little impact on patient care; however, in contrast, a flash flood may force immediate and complete evacuation of the facility for a period of time as in the case in Houston, TX, in 2005. Also in 2005, Hurricane Katrina and Hurricane Rita caused irreparable damage to hospitals in New Orleans and Cameron, LA.

A major question that avoids a validated and definitive answer is “How prepared are the nations’ hospitals to deal effectively with catastrophic emergencies?” The private sector maintains approximately 90% of the nation’s healthcare delivery capacity, but has not followed the efforts of federal healthcare facilities to reduce vulnerability through design and construction. Despite their efforts, the federal healthcare sector has been characterized as the weakest link in the homeland security chain.<sup>1</sup>

The International Association for Healthcare Security and Safety (IAHSS) has developed the following basic industry security guideline relative to healthcare emergency management.

#### IAHSS—HEALTHCARE SECURITY GUIDELINE, #10.01

##### **Emergency Management—General**

**STATEMENT:** Healthcare facilities (HCFs) will develop and maintain an emergency management program to identify and address threats/hazards/emergencies that may impact the facility and its operations.

##### **INTENT:**

- a. A multidisciplinary team should be appointed to develop and maintain the emergency management program. The team should have express support of the facility’s CEO along with authority for the program.
- b. Security staff should have a clearly defined role in the HCF’s emergency management program.
- c. The emergency management program should be based on the four phases of mitigation, preparedness, response, and recovery.
- d. The facility should conduct a comprehensive hazard/risk vulnerability analysis (HVA) to identify and prioritize threats/hazards/emergencies that may impact facility operations. HVA should be reviewed annually and whenever a new threat/hazard/emergency emerges, preparedness activities change.
- e. Multidisciplinary emergency response plans should be developed to address the potential threats identified by the HCF.
- f. Emergency response plans should have an all-hazards incident command system (ICS). Emergency response plans should address not only immediate and short-term response by the HCF but also the possibility of emergency operations lasting for days, weeks, or even longer.

- g. HCF staff should receive education and training in emergency management consistent with their most likely role in responding to the event.
- h. Emergency response plans should be exercised both for training purposes—so staff understand their roles and responsibilities and feel comfortable in those roles—and to identify the plans' strengths, weaknesses, and areas for improvement.
- i. Emergency plans should include community involvement—other HCFs, emergency responders, and government agencies.
- j. Emergency plans should include provision for the care and well-being of HCF staff and their families.

**REFERENCES/GENERAL INFORMATION:**

- Hospital Incident Command System Guidebook, August 2006.
- Environment of Care: Essentials for Healthcare, 7<sup>th</sup> Edition, The Joint Commission, Oakbrook Terrace IL.
- National Incident Management System (NIMS) <http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf>

**Approved:** November 2008

### *Hospital Leadership*

The first steps in developing plans and programs to manage emergencies include the setting up of a work group (a multidisciplinary committee). This work group would include representation from the Medical Staff, Nursing, Risk Management, Facilities, Security, Safety, and others deemed appropriate. In the past the Director/Manager of Security was often the person who was given the responsibility to lead this group. Today, it is somewhat common for the hospital to staff the position of Emergency Preparedness Director. [Table 24-2](#) shows the results of a recent study of different hospital positions that have the leadership responsibility for the Emergency Preparedness Program.

### *Phases of Emergency Management*

The TJC views emergency management in four phases that take place over a period of time. They are as follows: mitigation, preparedness, response, and recovery. The mitigation and preparedness phases generally occur before an emergency event, while response and recovery are phases that take place after the event. The details of activities and actions required relative to these four phases should be captured in the organization's Emergency Operations Plan (EOP). Once the EOP is completed, it must be tested through emergency response exercises and drills to evaluate its effectiveness. Thus, emergency management is an ongoing process of planning, directives, evaluation, more planning, added or changed directives, etc.

## Emergency Preparedness Drills

Emergency drills are required by TJC and other accreditation or regulatory agencies. Every accredited facility must conduct drills and prepare a written report evaluating each drill.

**Table 24-2** Hospital Position Assigned Responsibility for Emergency Preparedness<sup>2</sup>

Hospital Position	Percent of Survey Group
Emergency Preparedness Director	33%
Security Director	20%
Safety (Director, Manager, Office Coordinator)	13%
Facilities Management Director	11%
Risk Management Director	5%
Other	18%

People who have been assigned to observe specific aspects of the plan must meet after the drill to determine the plan's effectiveness. It is generally agreed that observers should be people from outside the organization when possible. They traditionally come from state agencies, offices of emergency preparedness, medical societies, or other medical care facilities. Drills serve a very important purpose, and they must be conducted with all the realism possible. It is extremely difficult, however, to rehearse certain parts of an emergency disaster plan when the facility is open and conducting routine, everyday business. One of the most difficult elements to practice is that of people and vehicle traffic control. It is not practical to restrict visiting or to turn away patients who have an appointment. Physicians and the community will not accept the curtailment of normal activities for a drill.

Real progress has been made in the last few years for healthcare providers to integrate their emergency management planning and operations with other community resources. This area-wide coordination has greatly improved the ability of a community, working together, to respond more effectively to the vast array of different types of emergencies both large and small. It is therefore natural to conduct emergency exercises and drills, both organization-specific and community-wide. There will continue to be more and more federal involvement in community emergency management through control of grants and legislation. An emerging federal program is the Homeland Security Exercise and Evaluation Program (HSEEP), which develops standards for hospital exercises. Many hospitals already use HSEEP methods to conduct their drills in conjunction with community public safety agencies.

An example of a large-scale mass casualty community drill was recently conducted by the University of Wisconsin Hospital and Clinics, which was dubbed "Operation Red Dragon." It was the largest mass casualty drill to be held in WI state history. Members of the 415th Chemical Brigade, of the US Army Reserve with 170 participants, and the urban hospital network were involved in the drill. Members of the brigade played victims and the hospital tested its state-of-the-art decontamination system. The primary goal of the exercise was to test communication between military and hospitals in the event of a large-scale incident.<sup>3</sup>

Another example of healthcare organizations integrating their emergency response planning with other community resources is the Special Operations and Response (S.O.A.R.) trailer as part of Carolinas HealthCare System (HCS), headquartered in Charlotte, NC. The trailer is shown in [Figure 24-1](#).



**FIGURE 24-1** The Carolinas Healthcare System Mobile Emergency Response Unit.

The specially designed 16-foot trailer was created to provide communications and tactical support to security, law enforcement, and firefighters at remote sites throughout the CHS service area. In addition to its onboard communications (HAM, UHF, VHF plus connections for standard/satellite phones), the trailer allows for recharging of radios, respirator batteries, and like equipment. Plans are to install additional equipment, which will have the ability to create ID badges onsite for personnel responding to the event.

## Incident Command System (ICS)

An ICS is a basic component of the HCF's EOP. An ICS is the combination of personnel, procedures, communications, equipment, and facilities operating within a common organizational structure directing the response and activities in managing an emergency incident or condition. There are two major models of incident command structures in use in the majority of US hospitals. One is the federal model, developed by the Office of Homeland Security, which is the National Incident Management System (NIMS), and the other, Hospital Incident Command System (HICS), developed by California's Emergency Medical Services Authority. The HICS model is specifically directed to hospitals for incorporating a command structure, defined responsibilities, and common terms. It should be noted that the original California model was named Hospital Emergency Incident Command System (HEICS) and in 2005 the word Emergency was dropped to become HICS. The NIMS model is a somewhat broader model (nonspecific to type of industry or organization) of practices in emergency preparedness and response to a national framework of managing critical incidents. There have been recent changes in the HICS model to more closely align, yet to be hospital-specific, to the broader NIMS model.

*NIMS and Federal Funding*

An important element of NIMS is their publication, “FY 2008 and 2009 NIMS Implementation Objectives for Healthcare Organizations.” Federal grant funding for hospitals through Assistant Secretary for Preparedness and Response (ASPR) and Health Resources and Services Administration (HRSA) require meeting a minimum number of the NIMS objectives (activities).

There are 14 NIMS objectives for healthcare organizations (FY 2008 and 2009) that are grouped under five major categories. These categories are

- Adoption (of NIMS);
- Preparedness Planning;
- Preparedness Training and Exercises;
- Communication and Information Management;
- Command and Management.

## Primary Manmade Emergency Events

### Fire Prevention and Control

Security along with facility safety services has a major responsibility in fire prevention control regardless of whether a fire is manmade or accidental. Fires in US HCFs have decreased in the past decade; however, some 10% of HCFs have suffered a fire loss at some time in their history. Although this is a much lower rate than that of general industry, HCF fires can mean the loss of human life as well as significant financial loss. The term *fire prevention* refers to the everyday activities that eliminate hazards and prepare people to react properly should a fire actually occur. In this discussion, the term “fire control” pertains to the basic organizational reaction to an actual fire. Both fire prevention and fire control should be addressed in the organization’s fire safety plan.

Patients being treated range from those who can move freely without help to those who cannot be moved without life-support equipment. Also, infants, children, behavioral health patients, and the elderly present unique requirements that must be considered in the fire plan. The elderly, especially those in nursing homes, are a particular concern. More deaths occur each year in facilities that care for the aged than in all other healthcare facilities combined. Not only are these facilities minimally staffed, but a high percentage of the elderly must be assisted during evacuation. The aged are generally slower to react to emergencies, and they often react unpredictably. An additional complication is that the products of combustion, even in small quantities, are often more fatal to older people.

*Fire Safety Programming*

A fire safety program can be viewed as five basic elements: (1) prevention, (2) detection, (3) containment, (4) evacuation, and (5) extinguishment. These elements chronologically define a standard organizational response to a fire threat.



### *Fire Prevention*

Prevention encompasses the activities of the fire safety program that occur before an actual fire, including the identification and correction of fire hazards, fire control planning, employee and occupant education, design and specifications, equipment tests, drills, and fire department liaison. Absolute fire safety is unattainable because it is impossible to exclude from the facility everything that burns and all sources of ignition. Facility inspections are conducted by all kinds of inspectors, including representatives of insurance companies, CMS, TJC, city building departments, state and city health departments, and fire department personnel. Some of the best inspections, however, are those conducted by organizational personnel. If they are conducted properly, a continuous, everyday fire inspection program is accomplished. Security officers on their rounds should note and/or correct fire hazards they see or that are brought to their attention by others. Security officers on rounds should be particularly alert for people smoking in prohibited areas. Officers should correct and report doors left open that should be closed, obstructions to egress paths, careless use of oxygen cylinders, and other fire safety violations. If a hazard cannot be corrected on the spot, officers can, through proper reporting, initiate administrative action.

### *Detection*

Automatic early warning smoke detection and pull box systems are typical in many facilities since regional and national codes generally require this equipment for inpatient facilities. In many healthcare facilities, detection equipment transmits a signal directly to the fire department, while at the same time alerting facility personnel. Smoke detectors use sensing units that respond to the presence of products of combustion that result from a fire. Other types of detectors may respond to heat or flame. When the threshold is exceeded, the sensor is activated. Most HCF fire detection systems use a combination of devices due to the varied situations the medical care environment presents. Activation of a fire detection device may also control various items of equipment; it may activate fire extinguishing equipment and air-handling machinery, send elevators to predetermined locations, and release magnetic hold-open devices on doors.

### *Containment*

The third element of the fire safety program is the containment of smoke and fire. The objective is to contain the fire in the room or area of origin. When this is not possible, the goal is to provide successive levels of defense or areas of refuge from the fire. The five basic areas of fire containment are sometimes referred to as the *unit concept*. The units are the room, the compartment, the floor, the building, and the exits, all of which have a distinct function in the fire protection features of the building.

- *Unit 1.* The room—the smallest unit—is the first line of defense. The function of Unit 1 is to provide the first barrier against the passage of smoke. The more effectively a room can be sealed, the better job it will do in containing fires.
- *Unit 2.* The compartment is the second level of defense. The intention is to provide at least two areas of refuge on every horizontal plane of the facility. When an area

must be evacuated, the initial movement is horizontal rather than vertical. The Unit 2 compartment is created by smoke and barrier walls.

- *Unit 3.* The floor, or floor assembly, is the next level of containment. The function of the floor assembly is to prevent the spread of fire and smoke from one floor to another.
- *Unit 4.* The building is the fourth level of protection. For the building to remain structurally intact for a period of time, it should maintain structural components that offer minimum contribution to any fuel load and that can withstand the effects of a fire within the facility.
- *Unit 5.* The exit path is the final unit in this concept of fire protection. At least two remote exits must be provided on each floor or fire section of the building. Exits need not necessarily lead directly to the outside. They can include egress to interior stairs, exterior stairs, horizontal exits, ramps, and exit passageways.

Fire containment can also limit the air needed to sustain combustion. The heat and smoke from a fire generally rises as a result of the buoyancy created by the heated gases. The smoke and heat will also seek out a path to the outside air. If they cannot continue to rise, the smoke and heat will descend back to the floor level.

#### *Evacuation (Relocation)*

The fourth component of the facility fire safety plan is relocation of patients, visitors, and staff. The Life Safety Code—through its standards for exit capacities, types of exits, travel distance, door specifications, and similar details—ensures the necessary means of egress from a medical care facility during an emergency. It is the healthcare staff, however, who are responsible for moving any patients who are in imminent danger to a safe location. In hospitals, many occupants are incapable of self-preservation. This fact is recognized by the Life Safety Code, which places the main responsibility for patient safety on the HCF staff. Total building evacuation, as a measure of last resort, can and does occur. Patient relocation between smoke-protected compartments on the same floor is usually an adequate first step. Following the unit concept principle, the evacuation plan's first objective is to move patients to a safe compartment. At this point, it must be determined whether to continue horizontal evacuation or whether vertical movement (to another floor) is necessary. Wheelchairs and carts are useful and often necessary for relocating patients, but they may not always be available at the time and place of need. Blankets are always available, and security professionals generally agree that they can be the most important pieces of equipment on hand for evacuation. Elevators should receive special consideration in the fire evacuation plan. Generally, plans prohibit the use of elevators for egress or relocation purposes because of their recall features, which are normally activated in a fire condition. An elevator may stop at the wrong floor, exposing its occupants to the fire. On the other hand, high-rise hospitals present unique problems that may require the use of elevators for vertical relocation under controlled conditions. In addition, the fire department may need to utilize an elevator for their firefighting purposes. Generally a building of more than seven stories is considered a high-rise, and is the limit of most fire

department ladders. A vertical evacuation plan is mandatory for high-rise buildings. One or more elevators in a wing removed from the fire area may be used to transport patients to another floor much more quickly and with fewer possible medical complications than when patients are carried down a stairwell.

It is noted that not all evacuation of patients will be related to a fire situation. Evacuation for any number of emergency conditions such as weather disasters, loss of infrastructure support, bomb threats and such may require moving large numbers of patients. The unique operational issues of evacuation under different conditions should be covered in the organization's EOP. In terms of providing evacuation plans for different types of patients, the forensic patient must also be part of the planning effort.

### *Extinguishment*

The last element of the hospital fire safety program is extinguishing the fire. The suppression of fire by staff is achieved either manually or by automatic suppression systems required for all new construction. The automatic sprinkler system is the most common of the automatic suppression devices. The automatic sprinkler system also acts as an alarm device because all systems are installed with water-flow sensors that activate an alarm when water is flowing in the pipes. The sprinkler is activated by a thermally sensitive element that automatically releases water at a predetermined temperature. Other piped extinguishing systems include water spray, foam, carbon dioxide, dry chemical, Halon, and newer, environmentally sensitive, clean agents. The standpipe and hose system, found in most US medical care facilities, is used to provide quick and convenient water streams. This system is most generally used by fire department or trained fire brigade personnel. It is not uncommon to eliminate the hose at the valve locations. The rationale for this is that most fire departments supply their own hose. Further, there have been reports of vandalism by opening the valve a little, allowing the hose in the cabinet to fill slowly with water. The hand-held extinguishers used in medical care facilities are primarily two-and-one-half gallon, stored-pressure water extinguishers, carbon dioxide extinguishers, and multipurpose (ABC) extinguishers. The type of extinguisher at any given location is predicated on the primary type of hazard involved.

### *Employee Reaction to Fire Events*

Proper employee reaction to a fire is one of the fundamental factors in saving lives and property. Fire safety is a race against time, and the action taken within the first few minutes can make the difference between a minor fire threat and a tragic disaster. Because employees must act almost instinctively when fire breaks out, detailed instructions are seldom remembered. The following simple steps, expressed through an easily remembered acronym, are widely used in healthcare facilities: **R** *Rescue* those in danger. **A** *Activate* the alarm. **C** *Contain* the smoke and fire. **E** *Evacuate* and *extinguish*.

### *Fire Safety Training*

Any employee could be the one who discovers a fire or who is the first to arrive at the scene of an alarm. The high rate of personnel turnover in medical care facilities and

the difficulty of retaining procedures that are not used routinely require continuous in-service and new employee training classes. Fire safety training is usually the responsibility of the Safety Administrator. Training can include posters, contests, in-service training, and fire drills. One of the obstacles faced in fire safety training is that little uniformity exists among facility fire plans. Because of the transient characteristic of medical care staff, an individual may work at two or more facilities at the same time. Organizations and facilities all have unique characteristics that require special fire planning; however, especially within a given locality, common fire plan components among facilities would reduce training time.

#### *Basic Security Fire Response Considerations*

Security's role in a fire situation is part of the overall facility fire plan, which in summary includes:

- Ensuring that responding fire department personnel gain access to the facility complex, buildings, and internal areas. This may require unlocking gates or doors, holding elevators, turning on lights, and even escorting fire personnel to the fire area.
- Controlling traffic, including vehicular traffic and people on the perimeter of the fire scene as well as the emergency operations areas.
- Assisting with the evacuation process if necessary.
- Assisting emergency personnel throughout the emergency.
- Securing the area after the conclusion of the incident. A fire watch may be required for some time after the fire has been extinguished.
- Providing security officer fire training. This training goes far beyond the general employee fire training previously discussed. Security officers are not only the first responders in many cases. The action taken in the first few minutes will bear directly on the outcome. Initial concerns involve sizing up the situation for personal safety, sounding an alarm, containment, and controlling the fire. Beyond these basics, there may be evidence that should be protected or conversations that should be noted and retained. Arson does happen in medical care facilities. Security officers must notice if someone has an unnatural or unusual interest in the fire. In short, security officers may be exposed to much information in the initial moments of a fire—information that must not go unnoticed or it may be lost forever.
- Preparing appropriate documentation of the fire incident.

### **Bombs and Bomb Threats**

Bomb threats are a reality for medical care organizations. Although the number of threats has decreased over previous years, a significant number still occur. One of the unique features of the bomb threat is the guessing game it forces the threatened organization to play. Is it real or is it a hoax? Where do we search? Is evacuation necessary? These basic questions become the framework of the facility response plan. The plan must be flexible

to the degree that the information received can be applied to these questions at the time of the threat crisis. A bomb can be described as any explosive, incendiary, or gas-filled container. Many chemicals can be used to make a bomb, and most chemicals are easily obtainable. Dynamite can be purchased or stolen from construction sites. Ammonium nitrate is sold in stores that handle fertilizers. Potassium nitrate and black powder can be bought at shops that supply chemists or hunters. Pipe bombs are commonly used by amateur bombers. These bombs are made from an ordinary pipe capped on both ends and filled generally with black powder.

### *The Bomb Threat Plan*

All HCFs should have a written bomb threat plan. Each plan is unique to the specific facility; however, the basic steps of bomb threat programming can be categorized as follows: (1) prevention, (2) establishing authority, (3) receiving the threat, (4) searching for the bomb, (5) evacuating the building, (6) terminating the emergency, and (7) documenting the threat.

### *Prevention*

The first area of concern is the preventive steps that can be taken against a bomb situation. These steps are the same security safeguards that should be in everyday use to protect the organization against other security risks. In other words, the proper functioning of the day-to-day protection system is the first line of defense against the bomb threat. To be more specific, locking equipment rooms, switchboard rooms, utility closets, storage areas, and the like can help reduce the problem. Limited access, access controls, noting suspicious people and vehicles, and providing emergency equipment are all part of the everyday protection system.

### *Establishing Authority*

One of the most important aspects of properly managing a bomb threat is to specifically establish organizational authority. As basic as this point seems, it is a fundamental deficiency of many healthcare organizations. Authority and responsibility for handling the initial crisis must be designated to a position that is readily available 24 hours a day. Logical choices would be the nursing supervisor, the house officer, or the security shift supervisor. The various field resources brought into play during this type of emergency must know to whom they must report the information, and answers to questions must be immediately rendered. It may be necessary to activate the ICS to properly manage the bomb threat situation.

### *Receiving the Threat*

The bomb threat can be received in numerous ways. The most common method is by telephone, and the most common recipient of such information is the switchboard operator. Telephone operators and others who are likely to receive these calls should be trained to keep the caller talking as long as possible and to ask key questions, such as

where the bomb is, when it will go off, why it was placed, what kind of bomb it is, and other questions that may keep the caller on the line. The person who receives the call should make notes or activate a recording device. Not all threats indicate that a bomb has been placed somewhere in the facility. The threat may indicate a bomb “will be” placed in the facility. When this type of threat is received, access controls must be expanded and the organization may decide to examine property being brought into the facility.

### *Searching for the Bomb*

The bomb threat information received must be communicated to the designated authority within the organization, who in turn initiates the notification system. The first step in the notification procedure must always be to notify the appropriate law enforcement authority. In most cases, the law enforcement authority and facility management will decide jointly the type and extent of search required. It is not practical or possible to conduct an all-out search in every case. An all-out search includes everything from checking every patient’s belongings to removing all suspended ceiling tiles and all ventilation grille work. It could take at least a day or two to completely search a facility. It is presumed that people who carry bombs are well aware of the danger of premature detonation, and therefore in most cases they will want to get into the facility quickly and to get out even more quickly—which generally precludes an elaborate hiding process. If sufficient organizational personnel are available, the search should be conducted by staff rather than by the police or fire department. The proper role of the outside support agencies is to assume control if a bomb or suspected bomb is located. Employees should conduct the search for two basic reasons. First, staff are in the best position to know what belongs and what does not belong to a given area. Staff are more knowledgeable of the layout of the facility and either have the capability to enter locked or controlled areas or know how to obtain access.

The use of in-house personnel to search avoids unnecessary confusion and minimizes disruption. Patients do not welcome a police officer, or a security officer, searching their room at 2:00 A.M. The search can be emotionally upsetting, and the reaction could very easily be panic. Many experts believe that bomb threat callers are frequently interested in stirring up as much activity and causing as much disruption as possible. Thus, one objective of a bomb search is to carry out the search in a smooth, routine manner, while taking every threat seriously. In bomb threat situations, the administrative person handling the threat may decide to advise only selected staff and patients. In general, patients should not be told of the problem unless absolutely necessary. Experience has shown that patients often set off a chain reaction that is detrimental to the entire process. Patients may respond by calling their families. In turn, the family may decide to come to the facility or call the facility for detailed information. This reaction can tie up needed communications lines and hinder response capabilities.

Whether a search is full or partial, areas of responsibility must be assigned. In some plans, the search personnel are assembled as a group so that the search coordinator can relate to them the information received and assign specific areas to specific personnel. In other plans, this information is communicated by telephone or through a public address

system with a code term such as “Mr. Search” or “Code Green,” or via electronic means. A problem that must be taken into consideration is the staffing pattern of the facility. When all departments are fully operational, the facility can be more easily and quickly searched than when departments are closed and locked. During the nonoperational period, security, maintenance, and environmental services personnel may be assigned an expanded role in the search effort. Floor plans that have been divided into specific search areas are used in some facilities. Personnel are given a map of the area for which they are responsible. In other organizations, these assignments are made from an administrative checklist that defines the areas. However the parameters of the search are defined, the person responsible for searching a given area must always report back to the control center when the search has been completed. The primary concern is for personal safety rather than property. Thus, a threat at 11:30 P.M., when a minimal staff is on duty, may preclude searching all areas. It may be that closed areas such as food service, business and accounting areas, administrative offices, maintenance shops, medical record areas, and the like receive only cursory examination. The occupied areas of the facility should be searched more thoroughly. Some controversy exists over the use of two-way radios during a bomb search. It has been suggested that radios should not be used because a bomb might be constructed to detonate in response to the transmission of radio signals. However, most experts believe that this possibility is extremely remote. In almost all situations, the radio system is active before the bomb threat was received and would have already detonated the device. The benefits of two-way radios during emergency operations support their use unless specific information is received to the contrary.

### *Evacuating the Building*

If the search produces a bomb or a suspected bomb, the cooperative efforts of security and public safety agencies come into play. Facility employees should never touch a suspected bomb. The investigation and removal of any suspect object is the responsibility of the public safety agency. Security's basic function is to seal off the area and to commence evacuation if necessary. The decision to evacuate rests with the facility administrative authority working in cooperation with the public safety agency involved. The evacuation of employees from a given work area presents no serious problems. Any plan for evacuating patients, however, must take into consideration the magnitude of the problems involved in moving the helpless and the seriously ill and the medical complications that may result. The extent of the evacuation is another decision that must be made quickly, based on the specific situation. A safe distance for evacuation is generally considered to be a 200-foot radius from the suspected object, including the floors immediately above and below.

### *Terminating the Emergency*

An important part of the organizational reaction to the bomb threat is the decision to end the response. All people who were notified of the receipt of the threat should also be officially informed that the organization is resuming normal operations. In other words, the

activity generated by the threat should not simply be allowed to trail off. After the threat is over, environmental services, maintenance, and security departments should brief the next shift of employees in their respective departments. In the normal course of their activities, these employees may observe something of importance that was overlooked during the earlier official search.

#### *Documenting the Threat*

The last step in bomb threat procedure is to document the incident for future reference. This task is usually assumed by the security or safety department. Regardless of who prepares the documentation, it is the responsibility of the person in charge of the threat incident to make certain that this important task is completed. The security report generally focuses on recording the facts of the situation. An additional administrative report that critiques the bomb threat response may be appropriate. The analysis may reveal deficiencies that require plan modification or further employee education.

### Strikes and Picketing

A real test of a facility's protection plan comes when the facility faces a strike or picketing situation. A *strike* occurs when some of the organization's employees, commonly represented by one or more unions, refuse to work as a protest against a serious grievance or a failure to negotiate a mutually acceptable contract. *Picketing* refers to the placement of people around the exterior of the facility for the dual purposes of informing the public of alleged problems and curtailing deliveries of supplies and equipment. The primary purpose of a strike is to create hardships for the organizations, weaken their bargaining position, and resolve the dispute in favor of the protesters. The hardships may include disruption of patient care, intimidation of nonstriking staff, loss of revenue, damaged or stolen property, negative community reaction toward the facility, and injury to persons. An organization need not be unionized to become the focus of a picket line. Picketing may be set up as a result of a strike or for the purpose of attempting to force the organization to recognize a collective bargaining unit. The immediate effect of a picket line is that union drivers may refuse to cross the line to make deliveries. In the initial stages, nonunion drivers will often cross the picket line until threats are made or physical violence occurs.

#### *Strike Control Team and Strike Action Committee*

During a strike, an organization must have a unified command structure. The organization's chain of command dictates the position that will be responsible for strike control operations. The strike control team should operate out of a strike incident command center so that all employees and outside support groups know where to deliver information or seek direction. A strike action committee should be formed by the head of strike operations to represent the various operating units of the facility and to function primarily in the prestrike preparation phases. Once a strike is underway, the committee will rarely be needed; however, it may meet periodically as a communication tool to keep operating units advised of the situation.



### *Nonstriking Employees*

The nonstriking employees are the basic resource for continuing patient care and ensuring a successful conclusion to the labor action. It is extremely important that the administration support nonstriking employees in every way possible. On the day the strike begins, all nonstriking employees should attend a briefing meeting designed to update employees on logistical matters, exhibit the administration's support and appreciation of the staff, and reassure employees. The employees should be told to expect harassing telephone calls. These calls generally threaten not only the employees, but also their families if the employees return to work. It may be difficult for administration to talk about this situation because administration generally wants to avoid negative issues. However, forewarning employees can mitigate the initial shock of these types of threats. Nonstriking employees are also vitally concerned about the protection of their vehicles while they are at work. Because experience has shown that vehicles are a major target of strikers, this concern is certainly valid. High priority must be given to this protection responsibility.

### *Initial Stages of the Strike*

The first day or two of the typical healthcare-related strike are generally peaceful and uneventful. The strikers are in a fairly good mood and enjoy talking with one another. The greatest number of picketers is on hand in the early stages of a strike, except for major rally events when the union tries to show a high degree of support. Inside the facility, the staff's initial reaction is enthusiastic support for the organization. As the strike continues on, both picketers and staff will exhibit frustration, disappointment, and exhaustion. After a few days, when the facility seems to be functioning well, the strikers begin to wonder whether efforts are meeting objectives. Their reaction may be to step up harassment. Incidents of intimidation, property damage, and other problems sometimes begin to appear. Another tactic that may occur and will affect the facility is a secondary boycott by suppliers and vendors. This illegal activity usually occurs much later in the strike, but it should be anticipated during early planning.

### *Picket Lines*

A major purpose of the picket line is to discourage employees from crossing the line to report to work. When the picketers see that employees are not being sufficiently discouraged and do cross the line to work, confrontations sometimes begin to take place. It is at this point that threats and acts of violence often occur. Administrators and supervisory personnel should be on the grounds during shift changes to support arriving personnel and to observe any incidents that might occur. Employees arriving to work are encouraged when they see the upper echelon there to support them rather than sitting safely behind their desks. Most healthcare facilities have a built-in security vulnerability that can become an asset during picket activities: a multitude of entrances and exits. For the duration of the strike or picketing, as many of these access points as possible should be open for employee use. The more entrances that are available, the more difficult it becomes for the picketers to cover them all. The law states that picket lines shall not restrict the right

of people to enter and leave the facility. Despite this provision, thousands of incidents on record involve injury to people and destruction of property during picketing. In coping with this situation, it is a common mistake to assume that law enforcement agencies will maintain law and order. Unfortunately, for a variety of reasons, police protection is not always at its best at such times. The healthcare organization has a responsibility to provide for personal safety and to protect its assets. The security department will necessarily play a strong role in achieving this objective. Several days before the strike, there should be a thorough inspection of the exterior of the facility to remove signs and other items that could be easily vandalized. One item often overlooked is sprinkler heads—a favorite target for picketers. Security personnel are generally deployed at the site of the picket line to show nonstriking employees and others who cross the line a high degree of protective support. Security's additional responsibility is to ensure that picketers stay off facility property, to prevent accidents, and to document evidence of wrongdoing. It is recommended that security personnel assigned to the strike detail be unarmed. A security objective is to be present but to project a fairly low profile, indicating that no trouble is expected. The type of trouble that might occur will not be deterred or corrected with the threat or use of a firearm. Security officers should be briefed by the administration and legal counsel just before they are deployed to the picket line. The basic message this briefing should convey is that officers must be professional. They must keep their eyes and ears open and their mouths closed. The officers should be reminded that they are representatives of the organization, regardless of their personal feelings about the situation.

### *Record Keeping*

A step that must be initiated immediately when a strike or picket situation develops is to establish a strike control center. A major administrative mistake is to assume that the confrontation will not last long. This assumption makes it easy to ignore the central reporting and its record-keeping role until the organization is well into a prolonged strike. All information concerning activities and incidents related to the labor action should be reported immediately to the designated recording location. All supervisory employees should be given the responsibility of reporting all incidents brought to their attention. A chronological record of incidents, including complete details, serves a variety of purposes, not the least of which is collecting the data necessary for legal actions. A consolidated central reporting concept will also serve as a clearinghouse to verify or reject rumors and to readily assess the situation. An important tool in dealing with and documenting strikes and picketing—and one that relates very closely to the incident recording function—is the use of photography. The task of photographing the labor action should be an assigned responsibility. Because camera equipment is often antagonizing to picketers, it should be used in such a manner that a minimum of confrontation occurs. The organization's response to the labor action may require the unexpected expenditure of funds. Special arrangements may have to be made to procure supplies, obtain drivers and vehicles, authorize meals, use taxi services, authorize overtime, and the like. During times of strike, the customary management controls tend to be loosened. Specific guidelines

must be drawn up for these unexpected expenditures, and the individuals who authorize the use of funds must keep adequate records.

### *Maintaining Supply Lines*

If it is to continue to carry out its mission, one of the first and most important steps an HCF must take during a labor action situation is to maintain a supply line. In most instances, a supply line requires the procurement of additional labor and vehicles. If vehicles are obtained from rental or leasing companies, it is usually only a matter of time before the rental agency demands the return of their vehicles. This tactic can be countered to some extent by having individuals rent vehicles from various agencies for one-time use. This procedure also proves valuable in avoiding harassment because the newly rented vehicle can be used to pick up supplies without being followed and subjected to threats, damage, or driver injury. Before picketing begins, the organization should contact all suppliers who make deliveries to the facility. The facility needs to know if nonunion or supervisory personnel will be available to make deliveries. It is better to pick up the supplies directly from the vendor or to have the order shipped to a temporary receiving site than to have confrontations between picketers and truck drivers. When truck drivers refuse to cross the line, their action supports and encourages the picketers. Because it is impossible for the facility to pick up the thousands of items it requires, particularly during a prolonged strike, offsite receiving areas can become necessary. Offsite receiving points should be well-secured and generally require security officer coverage. Depending on the severity of the strike, the location of the offsite receiving point should be changed periodically. Organizations should consider using a truck parked in a vacant lot or other out-of-the-way place and simply off-loading from one truck to the other. If the loaded trucks are not brought to the facility the same day, security precautions are important. One HCF involved in a severe labor action had parked three trucks overnight in an abandoned section of a railroad yard, and all three trucks were fire-bombed. The picket line not only inhibits the free flow of deliveries but also affects the removal of items, particularly trash. An institution of any size will find that a tremendous volume of refuse can build up in a very short time. It is essential that facilities move quickly to dispose of this material or they may find themselves in violation of health and fire standards. Inspectors from various federal, state, and local regulatory agencies just seem to proliferate during labor actions.

### **Terrorism**

To many US citizens, terrorism was something that took place elsewhere—until the September 11, 2001 attack. Acts of terrorism, both internationally and domestically, continue to occur, albeit on a smaller scale. Those who claim to know, predict another large-scale attack on US soil in the near future. The federal government continues to release information on how it is becoming better organized and better equipped to handle both domestic and international terrorism. If one looks at the record of the Transportation Service Authority with ever-changing plans and directions, it would give one a time to pause relative to how well the government is prepared. The color alert codes seem to be

a fad in passing and little is heard in that regard, except in airport overhead announcements. It has been reported that the Department of Defense is gearing up to play a larger role in homeland security. Under their plan, three rapid reaction forces will be ready to assist state and local officials with large-scale emergencies by 2011. One is a 4,700-person unit built around an active duty combat unit stationed at Fort Stewart, GA.<sup>4</sup> This may sound good, but it is the prevention of an emergency rather than the reaction to it that is of prime importance.

A question that continues to be asked is, Are hospitals a likely target for a large-scale terrorist attack? As one might expect, there are varying answers to the question. Lawrence Likar, a retired agent of the Federal Bureau of Investigation, speaking at an annual meeting of the American Society for Healthcare Risk Management (ASHRM) at their 2006 meeting in San Diego stated that the threat to hospitals is very low. Others claim that hospitals are at a high level of risk, as one criterion of the terrorist attack is to create a horrific event. A large-scale attack on a large hospital, perhaps even a children's hospital, would no doubt meet the terrorist objective. The general consensus of professional security administrators, however, is that the probability of a terrorist attack on a hospital is in the low to low-medium range.

### *Weapons of Mass Destruction*

A topic receiving increased attention is that of weapons of mass destruction (WMD). Within the realm of WMD, there are five generally accepted categories of terrorist actions: biological, nuclear, incendiary, chemical, and explosive (B-NICE). Hospital emergency departments will generally be early, if not the first, responders. While military medical services may be a resource, in all probability they may not be mobilized in a timely manner to meet initial needs.

### *Biological and Radiological Weapons*

The type of terrorist weapons is always at issue. It appears that a terrorist attack is more likely to be the use of a biological weapon. Anthrax and other dangerous biological materials are found in nature around the world, while weapon-grade nuclear materials are not readily available. It would be much simpler to disperse biological agents than to manufacture a nuclear weapon.

There is a growing concern that a weapon of terrorists' choice may be a radiological dispersal device (RDD), which uses conventional explosives to spread radioactive materials. These devices, commonly referred to as "dirty bombs," are not classified as a WMD as they do not usually produce the mass casualties of a nuclear device. The detonation of an RDD device serves a three-fold purpose: a blast and fragmentation generated by the explosion; the dissemination of radioactive material; and the fear and panic generated in the targeted area.<sup>5</sup>

Hospitals do not present a large source of radioactive materials. These materials are in the form of powder (i.e., blood bank irradiator), wafers (i.e., gamma knife), and liquid (i.e., diagnostic uses). Even in limited amounts, the theft of radioactive materials from

these sources is a potential threat deserving of proper security safeguards. Since there is a real danger in moving radioactive materials, it is likely that the theft of such materials from a hospital may in fact be used to construct a dirty bomb for detonation on site (the hospital).

The Washington Hospital Center, in Washington, DC, has recently begun to install radiation detection units. These units will alert staff if someone enters the hospital, who is contaminated with radiation. It is reported that testing will ensure that the units will differentiate between dangerous radiation and radiation used in cancer treatments. The units will also trigger an alarm if someone attempts to remove radioactive materials from the hospital.<sup>6</sup>

The security safeguards applied against terrorist threats coincide with safeguards used against civil disturbances, i.e., an expansion of the elements of the day-to-day security system in place.

### Gang and Mob Activities

Gang and mob activities are different from riots and civil disturbances in that gangs and mobs generally focus on the hospital as the primary target of their actions. Medical care facilities have been the object of demonstrations, ranging from peaceful marching, sit-ins, the occupation of administrative offices, and the takeover of communications systems. The purpose of these demonstrations has been varied and has included such demands as free medical care and the reinstatement of terminated employees. These disruptive activities characteristically show a complete disregard for the rights of the medical care facility and for the negative effects on patient care. In general, hospitals prohibit the exhibition of gang colors or flashing signs. Most security professionals agree that a strong security presence and dealing firmly but fairly with gang members is the best approach. Too passive an approach usually escalates disruptive behavior.

#### *Planning for Gang and Mob Activity*

One of the most important points to consider when planning an organization's response to gang and mob activity is the policy on arrests. Specifically, will arrests be made, and who will make this decision? Once the police have been called, the facility must be prepared to sign complaints and to follow through in prosecuting demonstrators if the police are unable to persuade them to leave.

Of the many mob activities directed against healthcare facilities, a demonstration against the Beth Israel Medical Center in New York many years ago is of particular interest to security practitioners. A group of people demonstrating under the banner of the Health Revolutionary Unity Movement disrupted services, and the hospital sought and obtained a court injunction prohibiting demonstrations within the hospital. The decision handed down by Justice Mitchell of the New York Supreme Court clearly stated that a medical facility is not a public place, and its sole purpose is to render medical care and treatment, for which a tranquil atmosphere is required. The opinion also stated that the demonstrators were in error when they justified their conduct on the basis of their constitutional

right to freedom of speech and assembly. Although the case is more than 30 years old, other case law has supported these principles. Although the law supports medical care facilities in their defense against intrusion, injunctions take time, and facility protection still requires careful and detailed planning.

## Civil Disturbances

The outbreak of rioting in the late 1960s presented a relatively new protection vulnerability for healthcare institutions. Hospitals had previously handled mass casualties, but the influx of casualties from rioting created new complications for protection services, including:

- Confrontations between police and rioters that often continued into treatment rooms;
- Hostile visitors who demanded attention, disrupted activity, and destroyed property to obtain their objective;
- Direct attacks on the facility, including firebombs and in one case a siege of gunfire.

In short, HCFs ceased to be the neutral ground they had been in the past. During the 1970s, few, if any, civil disturbances involved hospital operations. In mid-1980, heavy rioting hit Miami, Florida. One hospital, Jackson Memorial Medical Center, was under siege for a few days as rioters burned and looted just outside the hospital's perimeter. Security professionals learned three things from these riots. First, police and fire protection services may not be available as assumed or even as promised. Many facilities suffered extensive damage and disruption because the municipal protection services were stretched so thin that adequate protection could not be furnished. Every protection plan should therefore be predicated on the assumption that no external help will be available. Second, employees may be sympathetic to the rioters and their cause. Employee sympathy may be manifested in the theft of drugs and supplies for use at first-aid stations set up by the rioters, or employees on duty may create disturbances within the facility in support of the rioters' cause. For example, a wastebasket fire was set in a stairwell in one reported case. Although no real damage resulted, the smoke created confusion and panic among patients and staff. Third, separate treatment areas for rioters and the public may be needed to minimize continuing confrontation.

### *External Protection Planning*

Preparations for minimizing damage to the facility and safely moving employees cannot be made at the last minute. Thus, the first step in riot protection planning is to survey the perimeter of the property. For example, this might be the time to recommend fencing the north property line to divert foot traffic from crossing through parking areas. Security administrators should also consider whether exterior lighting is adequately protected to minimize destruction, whether landscaping decorations or other external items should be removed, and how employee vehicles should be protected. The next step is to carefully survey the exterior of the buildings that will require protection. Access doors and windows

are of primary concern. Even though normal access points cannot be eliminated during normal operations, administrators must be prepared to quickly authorize restricted access when a riot hits. The time to make certain that doors are equipped with the proper hardware is before a riot occurs. Security administrators should select the access point that could be controlled best if only one entrance were to be operative. The best entrance is not necessarily the most accessible one. If the facility has an emergency department, two access points are generally required: one for persons seeking medical care and another for everyone else. Windows and other glass areas are primary targets for destruction. Break-resistant glazing material is commonly used for protection. Another method is to precut plywood and install brackets on the window frames to permit easy and quick installation. If no glass protection has been installed or if the protection is minimal, interior blinds or curtains should be closed. If beds are near a window, they should be moved as far from the window as possible. Exterior lighting must be reviewed to determine whether the illumination is adequate. More light is needed during rioting than is needed under normal conditions. Security administrators should also check to determine whether light fixtures can be modified to prevent damage. Generally, little can be done in this regard, but making certain that lights are not within easy reach is at least one step that can be taken.

#### *Internal Protection Planning*

The interior of the facility should be reviewed to identify critical areas that need additional protection. This additional security may be in the form of hardware, or it may require establishing a security post. Areas of obvious concern are electrical distribution vaults, emergency power areas, equipment rooms (including elevator penthouses), oxygen and medical gas systems, emergency exits, traffic control, and surveillance areas. Organizations should seriously consider placing operators on all elevators. By manually controlling elevators, traffic can be controlled more readily, and in a sense the elevator operators provide an element of security. If emergency security posts are necessary, every possible post location should be given an activation priority so that as emergency conditions develop, the posts can be activated in a logical priority. The protection level will expand and contract during a civil disturbance crisis according to the threat at hand. Fire extinguishers and communications equipments are essential for every post; access lists and special equipment may be needed at particular posts. Planning may indicate that a reasonable approach to providing communications at every post is to install telephone jacks at each location or the use of cellular telephones. Most facilities do not have enough two-way radio equipment available for a significant protection posture; however, this situation is improving with considerable grant money.

A command post is required for all types of emergencies. In larger facilities the central security post is readily adaptable to this function until the emergency incident command post is established. During the emergency, it is suggested that two or three security employees be assigned to a task force that will be immediately available to deploy upon receiving notification from incident command that an emergency response is needed at a specific location.

Small clinics and medical office buildings must take many of the same precautions and plan in the same manner as hospitals do. One advantage of outpatient treatment facilities is that they can be locked up and need not continue to operate. However, past accounts of riot damage have shown that unoccupied buildings receive considerably more damage than occupied buildings.

## Pandemic Event

In 2003 a major epidemic of Severe Acute Respiratory Syndrome (SARS) spread to infecting individuals in 37 countries around the world in a matter of weeks. The SARS event was a near pandemic but was effectively controlled before reaching the pandemic state.

Now the H1N1 Influenza A virus (also known as a swine flu virus) is spreading around the world and has been declared a public health emergency of international concern by the World Health Organization. The US Government has also declared the flu outbreak a public health emergency, which is the first step for providing resources and support to the states, including release of stockpiled antiviral medications.<sup>7</sup>

In terms of security considerations for the HCF, relative to an epidemic and pandemic event, is that law enforcement and public safety agency support may be available. Unlike other community emergency events, there is no real defined scene that requires emergency response field management by the law enforcement agency. Fire personnel, as part of an EMS response, may however tax their resources. The HCF security concerns will be directly related to surge groups and a basic medical treatment concern may be lack of staff.

Security response planning in relation to a pandemic should expect

- A surge of persons seeking medical care that goes well beyond the capability of the facility, resulting in disruptive behaviors, including violence and destruction of property.
- A surge of persons seeking information relative to both inpatients and outpatients.
- A surge of persons (family/relatives) seeking discharge of inpatients who are not patients with a diagnosis of the identified pandemic disease.
- The risk of loss of stockpiled drug supplies via the means of break-ins and violence.

An undisclosed off-site security storage site should be considered.

The possibility that such chaos, disorder, and destruction of property will result in the closing of the facility should be part of the EOP.

## Active Shooter

While there is a long history of shootings in many, many facilities, the major shooting events in schools and retail shopping malls have generated serious concern among security practitioners. Hospitals have also been the scene of “active shooters,” killing multiple persons in many incidents, but not in the same high numbers. There have been discussions and meetings concerning security safeguards, preventive measures, and operational



security procedures for dealing with such an emergency. There do not seem to be as many answers as there are questions. In most cases, there is little warning that an active shooter event is about to take place. In most instances of these events, the retrospective players point to early signs of trouble that should have prompted a preventive approach. It is easy to critique after the fact, but difficult to perceive what an individual (or individuals) will do in the future.

### *Staff Actions*

In addition to notifying security and law enforcement, when safe to do so, staff must quickly decide on options such as hiding, evacuation (escaping the scene), or taking action when face-to-face with the shooter. These options have been advanced for the mall/retail shooting events. They may not be that well-suited for patient care staff, who must do all possible to protect the patients as well as themselves.

### *Communications to Departments and Units*

When circumstances permit and the means are available, the best staff action is to seal themselves and patients off by closing and securing doors. This may mean barricading doors with whatever is available (i.e., furniture). In areas where there are no patients, fleeing may be an option if it is perceived safe to do so.

Most active shooter situations are beyond a practical security intervention, and the best course of action may be containment until police arrive.

In order to mitigate an active shooter event, the ability to communicate with departments and patient care units is essential. Forewarning allows for action options to be considered by staff. Overhead paging is a common method of communication with staff and the use of computer alerts is increasing.

It is probably redundant, however, the best organizational approach to preventing an active shooter event is to maintain a strong threat policy and procedure along with a strong day-to-day security system.

## Accidental and Natural Emergency Events

Natural disasters, such as snowstorms, tornadoes, floods, hurricanes, and earthquakes, frequently activate the facility EOP. All of these severe natural phenomena events can significantly affect healthcare operations to varying degrees. The concomitant problems generally involve failure of the electrical system, interruption of deliveries, lack of communications, increased demand for medical treatment, and the isolation of the facility. Fortunately, facilities are not always hit directly by these disastrous weather occurrences, and they can continue to serve the community's needs with minimal interruption of normal services if proper planning has been completed.

In many cases of severe weather conditions, handling of mass casualties is not required. The focus is on other problems, such as providing housing for employees who cannot leave; finding temporary shelter for people who have been stranded; maintaining

supplies, including food; and transporting essential personnel from their homes to the hospital. When a facility operates under emergency conditions as a result of a community disaster, a unique phenomenon is readily apparent. Everyone pitches in to do practically anything required. The petty jealousies and animosities of the everyday routine quickly disappear. Even student nurses who are normally restricted in day-to-day activities are given more latitude to do the things that need to be done.

In addition to severe weather conditions, there is a host of other events that will put the facility EOP into play. There are ever-increasing events concerning accidents involving hazardous materials that affect scores of people. Transportation accidents occur that require hospitals to provide extreme amounts of minor medical care to high-level trauma care. In terms of transportation accidents, the airplane event often comes to mind; however, of late there have been an increasing number of railroad type accidents. Construction accidents and structure failures are always possible emergency events that force hospitals into an emergency operational mode.

## General Administrative and Operational Issues

### Emergency Announcement Codes

The use of word, number, or color codes to announce an emergency condition to facility staff is virtually common to all hospitals. What is not common is the number of different color codes used and a common matching of a specific color to the type of emergency condition. The exception is the somewhat common codes of Adult Medical Emergency—i.e., cardiac arrest (blue); fire (red); and infant abduction (pink).

Numerous hospital organizations have studied the need for a standardized common code system. One of the best-known studies, culminating in a comprehensive 81-page report, was that conducted by the Healthcare Association of Southern California in the year 2000.

Another study of emergency codes was conducted by the Colorado Hospital Association.<sup>8</sup> They found a huge mix of different codes by just 59 reporting hospitals. An example of this mix is revealed in the bomb codes reported. There were 13 different codes:

Code 4	Code Orange	Dr. Search
Code 99	Code White	Mr. Search
Code Black	Code Yellow	Personnel Alert
Code Blue	Dr. Atom	Code Green
Dr. Orange		

There is little question that standardized codes would result in reduced training time, reduced misunderstandings, and the emergency response would be more efficient. Despite all the efforts of the various groups advocating standardized emergency codes, little progress has been made. One of the obstacles to gaining a consensus is that there

appears to be too many different emergency code conditions proposed. The aforementioned California code study recommended 11 different codes, which many healthcare professionals feel is an excessive number of codes. Consensus seems to be that the most practical approach would be to limit the number of standard codes to no more than five codes using color designators. As the debate continues, it is suggested that the three basic codes of blue, red, and pink be used as the basic system of emergency codes with individual facilities adding more codes if they are in fact needed.

When developing a code system, healthcare organizations should not use codes common to other types of organizations, such as Code Amber. Amber Alert is a law enforcement term and should not in any way be confused with a healthcare term that might sound similar.

## Facility Access Control

In the event of an internal or external emergency, it may be necessary to restrict access for persons entering/leaving the facility as a whole, or a selected area within the facility. The terms *surge* and *lockdown* are used frequently when developing the EOP. These two terms are often used without definition and sometimes out of context. The term surge used by a medical caregiver will often be used to refer to a surge of patients. The same term used by the security administrator will generally mean a surge of persons seeking treatment, visitors, curious onlookers, media personnel, etc. Likewise, the term lockdown can mean restricting entry, restricting exiting, restricting specific access points (internally or externally), or a combination of such access points.

In *Chapter 18, Electronic Security System Integration*, the need to be able to lock down the facility in a very short time was discussed. The concept of a two-stage lockdown plan was also put forward in this discussion of controlling access during an emergency.

The means to lock down all entrances of all HCFs has become a basic element of healthcare security systems. This important aspect of security has become a national standard practice and will soon become the national standard of care for HCFs treating inpatients and/or outpatients. A recent study revealed that 7% of US hospitals do not have the capability to perform a total lock down of their facilities. It was further reported that it takes another 20% more than 15 minutes to secure entrances and exits.<sup>9</sup>

In a Joint Commission Resources publication, the concept of a three-tiered approach was advanced.<sup>10</sup> Each healthcare organization should decide what emergency access control system will work best for its mission and environment. This decision must then be included in the facility EOP.

[Table 24-3](#) is a snapshot of the various levels of a facility access control system.

## Security Staffing Under Emergency Conditions

Perhaps the major challenge for the Security Administrator is staffing. EOPs often call for 8–10 times the number of security officer staffing requirements over the regular day-to-day staffing of the Security Department. In addition, the duration of the emergency can

**Table 24-3** Stages of Facility Access Control

Normal	Expanded	Stage I	Stage II
Operating Access	Access Control	Lockdown	Lockdown
The daily access points (internal and external) and controls by time of day and day of the week.	Access restrictions from the normal operating access plan. Pertains to general building access and specific internal areas.	A further restriction of access usually restricting entry points with specific designated points controlled by personnel.	Locking of all building access points with personnel assigned to each entry and/or emergency exit point.

vary from a few hours to days to weeks, requiring expanded security operations. Staffing also depends on the type of emergency. If the emergency is an external transportation accident, staffing will be somewhat easy, as organization staffing will at least be par and as organization staffing will at least be par and hospital staff willing to stay past their shift or come from home. If it is a pandemic situation, the number of staff on duty may be fewer than normal, due to employee absences, and it is much more difficult to convince off-duty employees that you need them to come into work.

There are several traditional methods of increasing security staff due to an emergency situation. They include preplanned volunteers from other departments and an arrangement with a contract security service if the security department is an in-house program—neither of which works very well. If the emergency involves the community, and if the hospital security program normally relies on any amount of off-duty police coverage, it will be difficult, if not impossible, to satisfy even a minimal amount of expanded security officer man hours.

An agreement with outside security services providers to provide staffing in an emergency would be directly related to the provider's ability to field such manpower. Again, if the emergency condition is a community emergency, the provider regular security customers may need extra coverage and the hospital will certainly be in a subordinate position.

An in-house security program that regularly staffs its normal deployment plan with all full-time security officers has a very difficult time maintaining consistent staffing without the use of excessive amounts of overtime. The utilization of a contingent group of part-time officers is a good practice and is helpful when expanded security staffing is needed.

## Mutual Aid Resources

Not all emergency planning will be done on a consolidated community-wide basis. Planning for any type of emergency, whether internal or external, requires close liaison with other medical care facilities in the community. The security administrators of healthcare provider organizations should meet regularly for mutual aid planning purposes. An important consideration in mutual aid planning is to join with organizations that are not likely to be involved in the same emergency at the same time. Resources of

one facility should be readily available for use in another facility. The planned exchange of resources—whether security officers, vehicles, cameras, etc.—should be organized, and each organization should sign a formal statement of commitment. These types of documents are often referred to as a *memo of understanding*.

## Security Uniforms and Marked Vehicles

In some assignments or functions, the identification of security personnel is a detriment. Planning should take into account that uniformed authority figures may sometimes create problems. Consideration should be given to certain staff wearing street clothes, i.e., drivers who may need to pass through disturbance areas. Drivers should carry a letter indicating that they are employees on official business. Marked vehicles and especially marked security vehicles may also become targets. The objective in using both street clothes and unmarked vehicles is to avoid calling attention to certain security activities.

## Employee Travel and Housing

Another problem that requires considerable planning is that employees may not be able to travel freely to and from work because of a curfew, police lines, or fear of harm. Experience reveals that even though employees may be willing to travel to work under adverse conditions, anxious friends or relatives often persuade them to remain at home. Curfew terms vary widely according to local conditions and objectives. A common restriction is to prohibit people under a certain age from being on the streets after a certain hour. When this condition was imposed in a major city, it created a problem for the hospital because many employees were affected. The solution was simple. In addition to their name badge, employees carried a letter addressed to law enforcement that was signed by the hospital administrator, and contained the employee's name and address, the time dismissed from work, and a statement that the letter was intended for use only for the date indicated. This approach worked well and was reported to be widely accepted by law enforcement personnel. When police lines are established, altered travel routes are an obvious course of action. When police lines surround the facility, some procedure must be devised for staff access. Staff identification cards or badges are one solution. Another approach may be for a facility representative to be stationed at a central point along the police line to verify employee status. Individuals who attempt to cross the police line can be identified with simple questions about their department, employee number, birth date, or other data. The facility representative will be able to verify many employees by sight. During a civil disturbance, organizations may encourage employees to stay on the premises for their own safety and for the purpose of maintaining an adequate staff. Employees sometimes insist on staying regardless of the official stance, and thus some planning for employee housing is mandated. An inventory of beds that can be used in an emergency should be maintained. A thorough review of a facility often uncovers more beds than expected. Beds can sometimes be found in classrooms, blood banks, on-call rooms, and electrocardiogram and electroencephalogram areas. In addition, cots

can be set up in many areas for temporary accommodations. To ensure the utilization of all beds and to keep a record of where employees are housed, assignments must be made by a designated facility representative. Employees should not be allowed to assume their own accommodations even in their own departments. When more employees request accommodations than are needed to work, a system of housing authorization by department heads may be necessary to maintain adequate control.

There will of course be additional administrative and operational issues to be defined and addressed by individual healthcare provider organizations.

## References

1. Blair, J.D. (2008, March/April). Are Medical Facilities Doing Enough to Prepare for Catastrophic Events? *Healthcare Construction & Operations*.11.
2. Weronik, R. (2008, January 21.) *Securing our hospitals: GE Security and IAHS healthcare benchmarking study*. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
3. University of Wisconsin Hospital Completes Largest Mass Casualty Drill in State History. (2009). *Emergency Management Alert*, HCPro, 8 (25).
4. Hsu, S., Tyson, A.S. (2008, December 1). Pentagon to Detail Troops to Bolster Domestic Security," *Washington Post*.
5. A New Breed of Threat. (2004, March). *Access Control and Security Systems*. 55.  
(Note: best information provided.)
6. Hall, Mimi. (2008, November 5). D.C. Hospital Installs Radiation Detectors. *USA Today*. 19A.
7. The H1N1 Influenza A Virus: A Test Case for a Global Response. (2009, May). *Rapid Public Health Response Project*. The George Washington University School of Public Health and Health Services. Washington DC. 1.
8. Colorado Hospital Association. (2008, July 23) Emergency Code Use in Colorado: Results from a Survey of Colorado Hospitals. Retrieved June 25, 2009 from [http://www.cha.com/index.php?option=com\\_content&task=view&id=959&Itemid=208](http://www.cha.com/index.php?option=com_content&task=view&id=959&Itemid=208).
9. 1 in 4 Hospitals Face Lock-Down Challenges. (2009, July 23). *Campus Safety Magazine*. Retrieved July 24, 2009 from <http://www.campusafetymagazine.com/News/Default.aspx?NewsID=3171>
10. Colling, R. (2002). Security Issues for Today's Health Care Organization. *Joint Commission Resources*, Oakbrook Terrace, IL.

## A Primer for Healthcare Executives

It is 6:00 P.M. on Friday, you are packing up for the weekend, but at this moment you are the administrator on-call. You get a call from your security director that there has been gunfire in the emergency department waiting area, two people have been shot, and the gunman has not been identified or located. He is believed to still be in your hospital.

What do you do? Your MBA training never discussed how to handle a major breach in security such as this event. The incident command training you went through last month talked about external relationships and mutual aid agreements the organization should have. You are firmly aware of how the hospital is expected by TJC to be self-sustaining for 96 hours in the event of an emergency or other natural disaster. The logistical planning to maintain compliance with that particular standard has been a major initiative for your healthcare facility. The quarterly infant abduction drills required of the Environment of Care Committee have been most informative in bringing awareness to that type of critical incident. The changes made to the new Code Pink response plan have been met with good success. The \$200K capital investment in digital video surveillance and monitoring equipment last year brought a new emphasis on the importance of security to the organization. During the presentation to the finance committee, a commitment was made to continue to enhance protection levels within the organization by senior administration. In short, much has been done and all for the right reasons. Unfortunately, it just does not seem germane to the situation that is allegedly occurring at this moment.

The incident above could happen at any healthcare facility and has. The news is chock full of horrific stories such as these. In April 2009, a hospital worker, after having recently been downsized, shot and killed two employees and then killed himself at Long Beach Memorial Hospital in California.<sup>1</sup> In June 2009, Rhonda Stewart got into an argument with her estranged husband in the intensive care unit at the Charleston Area Medical Center's Memorial Hospital in West Virginia. She was asked to leave by the hospital staff. She later returned with a gun and shot him in the head.<sup>2</sup> In July 2009, an employee arriving for work at East Texas Medical Center in Tyler was shot three times by her ex-boyfriend before shooting himself.<sup>3</sup> The events listed above are just three events that occurred in a 4-month period. None of these healthcare organizations is an inner-city location surrounded by high-crime neighborhoods. They are a reflection of the average size and type of acute care hospital that could be located in any community.

But this is not the only type of violence your healthcare staff are experiencing. Your care providers are facing more verbal abuse and random acts of violence committed against them by patients and to a lesser extent, visitors, than at any other time in the history of modern medicine. In a 2007 survey conducted by the Emergency Nurses Association, 9 out of 10 Emergency Department Managers cited patient violence as the greatest threat to department personnel.<sup>4</sup> The physicians and nurses who staff emergency departments are demanding greater protection by hospitals. In the survey, emergency department nurses reported:<sup>4</sup>

- Dissatisfaction with the overall level of safety from workplace violence (89%).
- Feeling unprepared to handle violence in the ED given their education and training (83%).
- Reduced job satisfaction due to violence (74%).
- Impaired job performance for up to a week after a violent incident (48%).
- Taking time off because of violence (25%).

In the past decade progress in providing safe and secure healthcare environments has paled in contrast to other major business segments of our society. While the tragic events at the World Trade Center on September 11, 2001, jump started improved security for most US organizations, the event had little overall effect on improving healthcare security. Since 9/11 serious crimes such as homicides and serious assaults have steadily increased in virtually all healthcare environments.

Fortunately, today, healthcare has been given a relatively free pass by the media when major breaches in security occur. Take, for instance, the March 2008 shooting spree at Doctor's Hospital in Columbus, GA. A gunman allegedly distraught over his mother's dying at the hospital in 2004 brought three handguns to the fifth floor and shot a nurse and an administrative assistant, before gunning down a patient waiting outside in the parking lot. Outside of local community and state media coverage, there was minimal attention brought to this horrific incident by the national and international media. During the same week, an infant was abducted from Central Florida Regional Hospital in Sanford, FL, which received national attention due to the live media footage captured when the abductor was pulled over on the highway and the infant successfully recovered. However, many other similar security breaches have received little to no media attention. Thus public opinion has not been overtly influenced.

The public expectation of security inside a healthcare facility, which is largely formed by the media, is much different from the aviation and education sectors. Have you ever asked yourself why? We provide a room for our patients who must stay overnight in a room without a door that locks. We provide pain relief with powerful narcotics that induce sleep, mental uncertainty, and an unbalanced state of consciousness. We remove patients from their clothing and ask them to wear patient gowns that, let us admit, we would personally rather not be seen in. In short, our environment creates a number of basic vulnerabilities for our patients so that quality care can be administered.

The lack of media attention to the violence and other security concerns present in the healthcare environment will not continue perpetually. Healthcare professionals from



many disciplines believe our industry is one major security incident away from attracting the same scrutiny as the aviation and education industries. And with it, public opinion of what security safeguards should be employed in the healthcare environment will change. Are you ready and should you get ahead of the curve now?

No healthcare security professional is asking for greater media scrutiny, mind you, or the quality of care to be altered. Nor are we asking for greater administrative or regulatory oversight for security from either TJC or the Centers for Medicaid and Medicare. The basic mission of the organization to deliver quality care is well understood. The mission of your security program should be to provide a safe healing environment in which quality care can be administered.

The need for increased security has provided an unprecedented challenge in the methods and philosophies regarding protection of our healthcare organizations. Their safeguarding cannot be completely dependent on the security department. Many aspects of protecting healthcare organizations reach far beyond the control of the commonly accepted elements of a healthcare security department. Today, in order to achieve a high level of security, managers, top executives, and boards of directors must be more involved, through appropriate funding levels, and strong administrative direction with managing and supporting security issues. As leaders, we need your involvement and ownership of the protection effort in your day-to-day management obligations.

In this chapter, we do not wish to use scare tactics to change your expectations of your security program and how you resource it. Just the opposite; we want to enlighten you, the healthcare executive with a broad understanding of the security risks that are prevalent in the healthcare environment. Our goal is to help you make an informed decision about how to reasonably protect your organization.

We will ask a number of rhetorical questions to help enhance the posture of security throughout your organization. Emphasis will be placed on helping you, the healthcare executive, reduce the risk of adverse events that negatively affect the real and perceived nature of safety in your facility and on your campus. Discussion will include how the security program is designed to keep patients, visitors, and staff members safe and what must be done to create an environment where healing can occur safely while maintaining a welcoming environment.

## What Basic Objectives Should We Have for the Security Program?

Security programs must be structured to protect the healthcare organization within the restrictive factors of organizational mission, vision, and core values; physical design; patient and community demographics; employee and public relations; budget and resource availability; and the operational requirements of the facility.

Basic objectives of the healthcare security program can be viewed as:

- Contributing to the overall mission of the healthcare organization in the provision of excellent medical care services.
- Preventing security-related incidents through a proactive system of security safeguards.

- Responding to security incidents in such a manner that property damage or injury to persons is prevented or at least mitigated through competent and timely actions.
- Creating a sense of confidence in the minds of staff, visitors, and persons being served that they are interacting in a reasonably safe and secure environment.
- Providing services and activities in a positive and effective manner that supports the goals and culture of the organization being served.

The planning and implementation of program elements to achieve these basic objectives are influenced by both internal and external forces. TJC has specific security standards and elements of performance for security. For the most part, this accrediting agency has established minimum floor standards regarding the protection effort and not much more. HIPPA rules, *Privacy* and *Security*, have provided requirements for how patient data must be protected and controlled. However, the rules are vague and do not explicitly address what safeguards should be incorporated. Without precedent-setting case law, many patient data protection practices and procedures construed to be a HIPPA violation or viewed as in compliance remain individual interpretations.

CMS has developed interpretative guidelines (or standards) that affect security's involvement in patient care—elopement (prevention and response), restraint and seclusion, and use of weapons. The reduction in the use of physical restraints with patients continues to be one of CMS's major quality initiatives. Unfortunately, CMS's guidelines and their reading have contributed significantly to the ever increasing volume of assaults against, and subsequent injuries to, care providers, security officers, and others who work in the healthcare environment.

With the development of *Healthcare Security: Basic Industry Guidelines* the International Association for Healthcare Security and Safety (IAHSS) has significantly helped move the healthcare security industry forward. These basic security guidelines provide a consensus approach to the basic fabric and direction of the structure of the healthcare security program. They are intended to assist healthcare administrators in fulfilling their obligation to provide a safe, secure, and welcoming environment while carrying out the mission of their healthcare organization. The Association publishes an annual booklet containing the guidelines; however, as these guidelines are subject to continuous review and changes, the Association website ([www.IAHSS.org](http://www.IAHSS.org)) contains the most current and up-to-date information.

The protection program and the philosophy and objectives of the principal security administrator have a strong influence on the posture of security. However, the organization and its leadership should provide the ultimate definition of the security system. Internally, four of the most important factors contributing to the success of the protection effort are the leader selected to oversee security, the reporting relationship of the security administrator, the customer service expectations of the department, and the buy-in from the administrative staff of the security master plan.

## What Leadership Characteristics Should the Healthcare Security Administrator Possess?

The success of the security program is largely the responsibility of the security leadership and a direct reflection of their experience, responsiveness, and commitment to protection and customer service. If these qualities are not found at the top, they are likely absent in the security staff.

A common error for many healthcare administrators is to view the protection effort within a healthcare facility as a law enforcement function. Although some common ground may exist between security and law enforcement, the security function must always be rooted with a service orientation (prevention, education, and public relations) and not based on a law enforcement focus. Individuals fulfilling the security leadership position should possess a background in security and understand how protection principles apply to the healthcare environment.

Security of the healthcare organization is a business function and requires leaders who can think strategically and act tactically. Today's healthcare security administrator must be technically competent and knowledgeable about security management and electronic security systems. The industry remains people-intensive—over two-thirds (73%) of healthcare security budgets are dedicated to staff resources.<sup>5</sup> This requires individuals who can effectively lead others while having a basic understanding of how to solve problems, set expectations, and hold people accountable.

Operating budgets and capital budget requests are under greater scrutiny and require a business-minded security administrator who can defend capital requests with a return on investment (ROI) mentality, and have the capacity to develop a 3- to 5-year security master plan.

In short, the healthcare security administrator must be able to lead himself/herself and the change necessary to improve the real and perceived nature of personal safety on campus. The protection professional must be able to effectively manage the dynamic environment of healthcare. This includes changes in the delivery of healthcare services, multiple campus environments, home care, hospice, and community clinics. It requires the ability to build relationships with others, specifically emergency departments and other high-risk or security sensitive departments that rely heavily on the safeguards provided by the protection department.

Organizations such as the IAHS have many educational programs, development activities, and best practice information to help build the core body of knowledge within the healthcare security leader. Individual certification for the healthcare protection administrator should be required within a year of eligibility. The Certified Healthcare Protection Administrator (CHPA) administered by the IAHS and/or the Certified Protection Professional (CPP) are the two most recognized certifications in the security industry. Healthcare organizations are continuously rewarded with high-performing protection programs and effective security leaders when they have placed preference on these supporting memberships and specifying these credentials in the hiring process.

It does not matter if the healthcare security management model is proprietary or out sourced; the leader selected to administer the security program must align with the leadership philosophy of the organization and be a fit culturally.

### Where Should Security Report?

A required component of the TJC Security Management Plan is to clearly specify the position that has the responsibility for security of the organization and has a clearly defined reporting level for this position. The hierarchical level in the organization to which security reports reflects the importance that administration places on the security function, and the organization's responsibility of protecting persons and property. The important aspect of the security reporting level is that it must provide the organizational authority necessary to properly carry out its mission. A practical consideration is that security should report to an individual who has both the time and interest in the security function. In short, there must be proper administrative support for a security program to be effective and productive. A common reporting level for security is the vice president (or director) of facilities or the risk management administrator who, as a generality, seems to fit the foundation criteria for a successful program.

### What Customer Service Expectations Should Be Established for Security?

The successful healthcare security program incorporates the principles of good customer service. The security staff should be a direct reflection on the healthcare administrator's commitment to quality and customer service.

Great customer service and security service should blend together for the collective good. The historical perspective of security and customer service being polar opposites is no longer acceptable.

More than just security, security staff members should be ambassadors for the organization they serve and be expected to practice the rules of customer first and courteous enforcement. Their image, actions, and interactions with patients, visitors, and staff should leave an encouraging feeling about the hospital and the perception of personal safety. This will include being available to answer questions, providing directions and escort service, and serving a general purpose of being a "walking around" information desk.

### Why Do I Need a Security Master Plan?

A security operation cannot be superimposed, like an umbrella, on a healthcare organization with any degree of effectiveness. Rather it must be integrated into the routine operations of the organization.

A major intent of the security master plan is to provide the mechanisms and philosophy of achieving the overall direction of the protection system agreed upon by the stakeholders. It should be reflective of guiding beliefs and align these with daily practices

in the protection program. A strategic plan for security, it should be developed to set the philosophy and direction of the protection program for a longer term (3–5 years). The plan should include elements of financial planning and be sensitive to the overall demographics of the healthcare organization. It should also explore opportunities for building synergies with other departments and outside agencies. The major components of this plan are:

- Organization-wide security coordination and control;
- Neighborhood stability and security/crime prevention involvement;
- Public safety agency coordination;
- Criminal justice system interface;
- Organizational philosophy regarding the type and extent of physical and electronic security safeguards to be utilized;
- Degree of employee/staff involvement in the protection program;
- Building configuration and design considerations.

The underlying security philosophies that are put into place by the healthcare facility should not be developed in a vacuum by the security administrator. They should include key constituents of the organization to include leadership representatives from the emergency department, IT, human resources, facilities, and risk management. However, in the end, the healthcare administrator must support and give approval—designating the responsibility, providing authority, and allocating the resources necessary to implement the security program.

The security strategic plan will be unique to each specific organization as to form, format, and subject area. This plan, however, is necessary for all organizations to provide clear program direction. Without the framework of strategic security policy and infrastructure, a program simply becomes one of day-to-day reaction, often resulting in a nonproductive and costly effort. The security master plan, in its final format, affords additional protection as it helps document the why behind what is being done in the protection program. The plan should contain an element that comprehensively documents all that has been done to enhance the posture of security. In the event of an adverse situation, the protection afforded by this alone is significant. In the end, the security master plan demonstrates the importance that security is taken by the highest levels of leadership in the organization.

## How Do We Identify Our Security Risks and Vulnerabilities?

All healthcare facilities, regardless of size, are subject to basic security risks. The range of security risks is extensive, from assaults and dissident group actions (demonstrations, civil disturbances, sabotage, and labor actions) to identity theft and loss of critical information. There are a whole host of other security risks that are inherent to providing patient care services such as drug theft/diversion, infant/pediatric abductions, medical imposters, and workplace violence.

The foundation of a healthcare organization protection system is the identification and assessment of the types of threats and the degree (impact) of damage if the threat becomes an actual occurrence. The identification of specific risks generally begins with a facility security review process, often called the Security Risk Assessment.

The identification of the magnitude of security threats or risks, along with their potential impact on the healthcare organization, is but an initial step in protecting the organization. The objective of the security assessment is to identify the security exposures so that a comprehensive, effective, and cost-justified security plan can be developed and implemented. Analysis and evaluation of the risks provide the rationale that security measures (safeguards) are implemented appropriately based on protecting critical resources while accepting a calculated degree of risk. It is understood that an asset cannot be protected completely without extravagant cost or unduly inhibiting the primary mission of providing efficient and quality patient care. The goal of implementing counter-measures for security risks is to make it difficult for a security breach to occur—to harden the facility as target. The level of difficulty to be implemented depends on the value of the asset and the organization's tolerance for risk.

There are a great many methodologies and formats that can be utilized to assess security risks and to measure the severity of those risks. There are two basic principles to keep in mind regarding security risk assessments:

- The methodology should not be overly complicated and the bottom line is that risk level conclusions are largely subjective in nature in terms of probability.
- A formal security risk assessment, conducted on a periodic basis, is simply a baseline that can and should be modified on an ongoing basis.

Virtually every security incident provides an opportunity for lessons learned which may affect the assessment. Changing neighborhood dynamics and renovation and construction projects are also among activities that may have a bearing on the security risk analysis. Additionally, new and modified patient care programs including changing space allocations are important to consider.

All security program safeguards should have some relation to the level of threat.

Once the process of risk assessment has been completed, an abatement plan has been devised, and safeguards have been blended into a security program, this process should begin again. The identification of security vulnerabilities and risks is ongoing. Risks previously identified may no longer exist, and new risks may appear as the dynamics of a healthcare environment continually change.

## Does the Community Standard Have a Role?

Gaining knowledge of the protection safeguards deployed at other healthcare facilities is an important consideration for every healthcare administrator. The community and patient demographics differ by facility; no two healthcare environments are exactly alike. However, physicians often have privileges at multiple hospitals and healthcare has a large

transient workforce who frequently job hop in search of better schedules, shorter commutes, and safer work environments. The knowledge of the model of security in place at other healthcare facilities alone can help mitigate a negative perception of the protection efforts on campus.

## The Security Staffing Model: How Large a Staff Is Needed?

The security force is often viewed as the quality linchpin in a healthcare facility's security program. Often, security officers are among the first people patients and visitors see and communicate with. They should create positive feelings about the facility and enhance the perception of safety within the organization. In short, the healthcare protection program needs reliable and professional security officers, not just security guards.

The numbers and types of security personnel required for an efficient security program is a fundamental question for every facility. It is not as easy as applying a simple formula using the square feet of buildings, campus acreage size, number of beds, number of employees, comparisons to like facilities, or any other profile data. It is indeed an individual facility question since the numerous factors that must be considered vary in depth and scope from organization to organization. To arrive at the required number of security personnel, it is necessary first to analyze and understand the security mission, determine the level of the organization's security risks and vulnerabilities to be managed, review electronic and physical safeguards planned or in place, and identify the various services to be rendered. The next step is to design a program that will support the mission, properly manage risks, and implement the intended services. Only then can the number of staff required to operate the program be determined. In short, determining the right sized security force takes a great deal of time, effort, and in-depth evaluation.

Healthcare organizations commonly make the mistake of hiring a complement of security officers and then determining what activities they will perform. In a similar vein, some security planners answer every security problem by suggesting the hiring of additional personnel. More people are not always the answer, and in fact, numerous security programs have been upgraded by reducing personnel through improved management, specialized training, and the application of new preventive security concepts. Unfortunately, sound planning and valid program justification often yield to that of emotions and easy solutions. In reality, more security personnel have been added to existing programs more because of poor response to breaches in security or distressing incidents than to sound planning.

The objective method of determining how many security personnel are deployed is first to determine the functions and the activity to be accomplished. Reference to the number of personnel required is a rather inexact measurement. Security staff should ideally be deployed on the basis of objective criteria such as those listed in [Table 25-1](#).

Security resources should be prioritized relative to business risk and the impact on quality patient care. Expenses associated with security staffing levels must be managed and balanced against the constant pressures of cost containment. The security staffing plan should not be viewed as a total FTE count allocated to the department, but the

**Table 25-1** Objective Criteria for Security Staffing**Security Staffing Criteria**

Total Occupied Square Footage	Campus Acreage
Primary Service Area Population	Scheduled Routine Functions of Security
Criminal Environment Analysis	Scheduled Special Functions of Security
Patient Volume (adjusted patient days)	Experience with Aggressive/Assaultive Behavior
At-Risk/Vulnerable Patient Population Served	Security Incident History (Internal and External Crime)
At-Risk Patient Involvement	Ratio of ED Visits to Security Patient Assists
Facility-Specific Unique Issues	Trauma Designation Level
Physical and Electronic Safeguards Deployed	Emergency and Service Response Time Expectation
Response Capabilities of Police	Weapons History at the Facility
Total Number of Public Access Points	Lost Time Injuries Related to Security Incidents
Security Sensitive Services Rendered	Politically Sensitive Affiliations

complement of staff stated to be on duty at any given time per the master schedule. The volume of security employees needed to fulfill the master schedule must be determined based on a ratio that considers the amount of unproductive time afforded by each security staff member; i.e., required training, absences due to vacation or sick, etc.

The protection program should refrain from flexing security staffing for temporary convenience or budgetary constraints. Absences and vacancies must always be filled unless uncontrollable circumstances exist. In lawsuits for inadequate security (e.g., a visitor assaulted in the parking garage), the risk associated with the FTE count model is a plaintiff's attorney claiming: "if there were three security officers as designed, there is significant propensity that the deployment of that officer could have prevented this crime from occurring." This argument adds credence to the dispute of inadequate security and often results in a higher negotiated settlement if the case is not taken to court.

Two factors that should not be left out of the equation in determining the number of officers required are the skill level and degree of productivity of each security officer. A well-trained security officer who looks the part, knows and understands his/her role, and consistently performs at a high level is much more productive than a guard who is not properly trained, supervised, or engaged in his/her protection responsibilities. Many healthcare protection administrators agree: one professional security officer can accomplish more than two security guards. A competitive compensation strategy coupled with a professional security officer training and development program are key strategies for obtaining a high level of engagement and consistent performance.

### Security Training: What Should I Expect?

A well-trained security force is the basic component of the healthcare protection system. Professional security officer training is a combination of protection, customer service,



and public relations. Proper training of security officers can produce the ROI in terms of helping the healthcare organization attain the highest level of security and safety.

Litigation has been a powerful driving force in the increase in healthcare security officer training. Claims that healthcare organizations have failed to provide necessary training are used with much success in lawsuits, especially those involving weapons, physical force, false arrests, and civil rights issues. The responsibility for the adequate training of security staff rests squarely on the organization.

Ironically, although a trained security officer can be at least twice as productive as a well-intentioned untrained officer, it is usually easier to obtain money for an extra position than for additional training. The number of security personnel is often mistakenly used to determine the level of protection regardless of the training required of or provided for the position.

Leadership development activities cannot be lost in the healthcare security training program. It can increase the effectiveness of the supervisors, managers, and directors involved in the healthcare security program and be the source for driving higher levels of both patient and employee satisfaction. Helping security leaders at various levels develop the skills and knowledge they need to succeed in their leadership positions can make the organization a better place to work and help the protection program retain its most critical asset—their employees. Many healthcare organizations have seen that investment in the development of its security leaders has a measurable ROI as it helps reduce costs in the areas of turnover, employer practice, and inadequate security liability. The IAHS is an excellent source for security leadership development and credentialing.

## How Do I Know My Security Staff Are Competent?

Security officers must be prepared to subdue a mentally disturbed patient, apprehend a thief, comfort a distraught mother, escort a lost visitor, and perform any number of other tasks at any time, anywhere in the facility. Training cannot be a one-time event. From the time they are hired and throughout their careers, security staff must continue training to learn, improve, and further develop their professional skills.

There are a number of state statutes that mandate how many contact hours should be provided for security staff training. Most educators, however, believe competency is a better indicator of a successful training activity. The amount of training time provided is not a good judge of an individual's skill level to perform the function of protecting a healing environment—their demonstrated competency is the best indicator.

A common question received from many healthcare administrators: What fundamental training elements should be required training for anyone fulfilling the role of security officer?

- *Security Role in Patient Care/Aggression Management:* Healthcare security officers can expect to be called upon to de-escalate and manage aggressive or violent behavior. Focusing on verbal de-escalation and voluntary compliance, the training should be designed to teach security staff members to successfully control aggression and other verbal or physically inappropriate actions of others in a medical care environment.

- *Use of Force*: Every healthcare facility should develop a use of force policy that includes the identification of situations, both clinical and nonclinical, in which security officers are permitted to use force. The new officers must be trained on the use of force policy upon hire and be provided specific training on each item of equipment they carry.
- *Restraint Training*: The basic requirement is that if a security officer is involved in the application of restraints, he/she has to be trained and demonstrate competency in the safe application and use of restraints.
- *Report Writing*: Of all the security officer's duties, the ability to write an accurate, clear, concise, and impartial security incident report is one of the most vital.
- *Customer Service and Security*: Healthcare security officers who perform their job correctly spend more than 50% of their time providing general services. As ambassadors for the organizations and the constituents served, the security officer must understand the rules of courteous enforcement and public relations.
- *Patrol Techniques*: The security patrol is the most common activity performed by the healthcare security officer. More than just walking around, the security officer must be trained to be "systematically unsystematic" to routinely change his/her patrol coverage. The new officers must learn that, while on patrol, they are looking for people in need of assistance or dangerous situations and how to use their senses.
- *IAHSS Progressive Certification*: Providing a foundational understanding of healthcare security, the Basic Training level is the first phase in the IAHSS Progressive Certification program. The Advanced and Supervisory Training levels expand on the Basic Training program and allow security officers to continue their education after becoming certified at the Basic Training level. The programs are designed for the healthcare security officer who desires to achieve higher levels of responsibility in the organization.
- *Other Training Considerations*: Many healthcare facilities provide training about security protocols and contemporary security topics such as those listed in [Table 25-2](#).

An often-neglected area of training is the operational aspect of the healthcare delivery system. Security officers should learn how various departments and sections of the healthcare system operate to understand better what they are protecting and their role in the delivery of quality patient care. The better officers understand the operations, the formal and informal hierarchy, and the history, objectives, and goals of the organization, the better equipped they will be to carry out their responsibilities.

## How Much Involvement Should Security Have with Patients?

Providing an appropriate safe treatment environment for all patients is a basic requirement of every healthcare organization. Clinical staff are expected to implement appropriate interventions, as needed, to prevent patients from harming themselves or others. Often this will include security officer support to provide constant monitoring to help

**Table 25-2** Contemporary Security Training Topics**Security Officer Training Topics**

Gang Awareness	Weapons of Mass Destruction
Infant Abduction Prevention and Response	Terrorism Awareness
Forensic (Prisoner) Patients	Emergency Preparedness
Very Important Patients	Active Shooter
Critical Incident Response/Scene Management	Workplace Violence Prevention and Response
HIPPA and the Security Officer	Disclosure of Patient Information
Media Relations	Laws of Arrest, Search, and Seizure
CPR/First Aid	Disaster Readiness

protect the patients from harming themselves, harming a care provider or others, or prevent the patients from leaving the facility.

There must be a clear understanding of how the security program engages with patients and their visitors within the healthcare environment in order to properly fulfill the security and organizational mission. The scope of expected assistance significantly affects security staffing decisions, the focus of security training, and staff expectations.

Responding to requests for assistance with patients is a valid and necessary function of any protection system. The security program that takes a hands-off approach to patient involvement is not fulfilling an important mission for the healthcare organization. Creating guidelines to govern the relationship of the officer with the assigned care provider and the patient with specific responsibilities outlined for the security officer is a must for every healthcare protection program.

An important element for every healthcare professional to understand is that any patient on a security watch is the direct responsibility of the nurse assigned to that specific patient. The nurse directs all action regarding the patient and cannot relinquish this responsibility to the security officer. The officer's involvement in this patient care procedure is merely an extension of the assigned nurse; all security actions with the patient are on behalf of the assigned care provider.

The frequency of security calls for patient assistance varies from organization to organization and depends on many factors, including the types of patients the facility serves and the availability of nursing personnel. There is a tendency for security to be called too frequently as demonstrated with a number of healthcare organizations that have witnessed their volume of security incidents for patient assistance more than double and the average amount of time spent for each event by security staff more than triple. The healthcare protection program should carefully monitor and measure their involvement in patient care for performance improvement by volume and total amount of time spent on average.

Most healthcare professionals agree that mental health patients are a significant factor in the explosive increase in the volume of security watches in the emergency

department and elsewhere in the healthcare facility. Many hospital emergency departments have responded by taking a page from the standard security practices employed in behavioral healthcare units. These practices include creation of a weapons-free environment, requiring all at-risk patients to gown, and training all emergency department staff in aggression management and de-escalation techniques.

### What Type of Uniform Should Security Officers Wear?

There are a wide variety of attire options available to the healthcare security program. A continuous debate is whether security officers should wear a traditional uniform (military or police style) or a softer look uniform that includes a blazer and slacks. The consensus is that security officers should never be outfitted in plainclothes.

The vast majority of healthcare security officers are traditionally uniformed. Wearing this style of uniform readily identifies security staff and commands control when it is necessary to regulate behavior and provides a deterrent to criminal activity. The uniform is versatile and worn indoors/outdoors and in all climates. This style of uniform is preferred for officers who encounter many confrontational situations or primarily perform foot patrol. The blazer style uniform with contrasting slacks (gray slacks and blue blazer) can be a very professional look, and works best for officers who work mainly inside the facility and function primarily in a public relations mode. Many behavioral healthcare facilities prefer security officers working in these environments to work in the blazer style uniform to prevent the uniform from unnecessarily antagonizing patients or visitors.

The type of healthcare organization, its customer service philosophy, and the primary function the security department in general is carrying out, or more specifically, the function of the security officer is fulfilling, should be the greatest influencing factor in determining the uniform to be worn by security staff. The officer with primary foot patrol responsibilities who should be highly visible will often wear a different uniform option from the officer whose primary function is greeting patients and visitor management.

### What Use of Force Options Should Be Made Available to Our Security Staff?

The use of force by healthcare security officers is sometimes necessary to maintain order and safeguard staff, patients, and visitors in a healthcare environment. The security officer must occasionally use a certain amount of force, from mere presence and verbal persuasion to physical intervention, to overcome resistance and ensure compliance with hospital policy and medical care plans.

For security program effectiveness and deterrent value, the preponderance of evidence supports healthcare security officers having additional tools at their disposal. These include some of the options identified in [Table 25-3](#). Whether security officers should be equipped with all, some, or none of these additional tools requires constant evaluation and reexamination. The answer is found in individual program needs and administrative preference to organizational risk exposure.

**Table 25-3** Use of Force Continuum/Options**Use of Force Options for the Healthcare Security Officer**

Officer Presence	The mere presence of a highly visible uniformed security officer, marked security vehicle, or K-9 patrol is often enough to prevent or deter crime or wrongdoers. Included in officer presence are standing, walking, running, and use of vehicle lights. Without saying a word, an alert security officer can deter crime or direct criminals away from a property by use of body language and gestures.
Verbal Communication	Used in combination with a visible presence, the voice can usually achieve the desired results. Words can be whispered, used normally, or shouted to be effective. The content of the message is an important as the demeanor. Most situations call for starting out calm but firm and nonthreatening. Choice of words and intensity can be increased as necessary or used in short commands in serious situations. The right combination of words in combination with officer presence can often deescalate a tense situation and prevent the need for a physical altercation.
Control Holds and Restraints	Certain situations may arise where words alone do not reduce aggression. Sometimes security officers will need to get involved physically. At this level, minimal force would involve the use of bare hands to guide, hold, and restrain. This should never include offensive moves such as punching, tackling, and choking. Medical takedowns could apply here, but only after ordinary holds fail to control an aggressive suspect.  Handcuffs are often used as restraint device if the security officer has been trained to use them.
Chemical Agents	Sometimes when a patient or suspect is violent or threatening, less-than-lethal measures are used in defense to bring the individual under control or effect an arrest. Before moving to this level, it is assumed other less physical measures have been tried and deemed inappropriate or ineffective.  Pepper spray/foam, OC spray are infrequently used in the healthcare environment, and only if the security officer has been trained on its use.  A distraction-based use of force, if used, should allow the security officer to get away, call for assistance, or subdue the individual. <i>It is important to note that many chemical agents may not be effective on mentally unstable, drug addicted, intoxicated, or hysterical persons.</i>
Temporary Incapacitation	To use force under this level means that the situation is so extreme, violent, immediate, and unavoidable that it is necessary to temporarily incapacitate an individual prior to arrival of police or other assistance.  Tasers (or other electronic control device) have increased in use in the healthcare environment for security officers who have been trained to use them.
Deadly Force	When there is fear of death or great bodily harm at the hands of another, a security officer is authorized to use deadly force in most states.  Firearms are most often used to fulfill this use of force option.

Every healthcare facility should develop a use of force policy that includes the identification of situations, both clinical and nonclinical, in which security officers are permitted to use force.

The use of force option made available to security officers is an important decision that must be made with deliberation and include healthcare administrative leadership team. There is always a risk; every use of force by security staff involves some liability and litigation exposure. The decision must be made on the basis of this question: *Does the use of force tool provide enough benefit to offset the liability and cost involved?*

While firearms can save the life of a healthcare security officer, they can also be dangerous to the person using them for protection. They can, and sometimes do, get into the hands of the opponent. A recent trend is for healthcare organizations resorting to alternative means of protecting security staff in the security program. At present, approximately 12% of US healthcare security officers carry firearms compared to 16% of security departments who arm their security officers with Tasers.<sup>5</sup>

Most healthcare protection professionals agree that the less-lethal use of force option provided by the Taser is better than the firearm to combat most escalated situations confronted by the healthcare security officer. Due to the fear of contaminating inpatient units, many hospitals prohibit the use of chemical agents in their use of force continuum. Additionally, most healthcare security programs prohibit nightsticks, batons, or collapsible batons as their use is often perceived as undue force.

Handcuffs are an important piece of equipment carried by many healthcare security officers. The devices can be very useful tools but their use should be documented and governed by the hospital's patient-restraint policy.

CMS is very specific about the use of handcuffs and other use of force tools in the patient-restraint process and although they do not outlaw their use, they do outline a specific response that includes immediate notification of law enforcement personnel. In short, CMS does not want to see the tools used in the patient-restraint process unless an arrest is imminent.

## How Should Security Be Designed into the Healthcare Facility?

Security staff members are the heart of healthcare security. There simply is no substitute for the professional expertise and human touch of security officers in the healthcare environment. However, carefully selected and properly applied physical safeguards and electronic security technology are playing increasingly important roles in protecting healthcare facilities.

While the basic physical security safeguards are still staples of security (barriers/fences, alarms, lighting, lock and keys), it is the electronic components of security that are experiencing explosive growth.

While many statistics point to a rather dire state of society, the hope for better healthcare workers' protection can begin with facility management/design. The healthcare administrator should require the security professional to work with hospital engineers,

project managers, and/or architects to incorporate the most operationally efficient and cost-effective security technology for the project and budget.

At the heart of this expectation is defining the specific security operating principles and philosophies of space utilization that drive specific technology application. The philosophy of all security design considerations should be to help build an environment that is patient-focused and incorporates both physical and psychological deterrence methods.

Realizing that physical controls cannot protect all things in all places, security professionals also use psychological deterrents, which are directed at the decision-making process of the individual. For the purposes of security planning, a psychological deterrent is defined as an individual's interpretation of a situation in which the potential positive or negative aspects of behavior serve to prevent or preclude the expression of that behavior.

The fundamentals of Crime Prevention through Environmental Design (CPTED) follow these principles as they include using the physical environment and other aspects of design to manage behavior. The proper design and effective use of the built environment can lead to reduction in the incidence and fear of crime as well as affect the behavior of people by providing physiological and psychological deterrence.

These low-cost/no-cost approaches to security should be a basic expectation and appropriately implemented whenever possible.

## How Important Is Access Control?

Forethought in the design to how access will be controlled to the environment is of paramount importance. The healthcare environment and hospitals specifically, by their nature, are designed to be open and accessible to the sick and injured and to family and friends. This means that criminals and other dangers can easily enter through their doors if not properly protected.

The main entrance in particular is a concern, as most hospitals specifically have very limited control of who comes and goes through this entry point during normal business hours. Access control, arguably the most critical aspect of healthcare security, requires the proper channeling of visitors and patients into and about the healthcare facility. The goal is to allow patients/visitors to move freely without feeling oppressed while at the same time protecting patients, visitors, and staff.

Good security design and electronic access control technology can significantly reduce this area of concern. Today's technological advancements in access control enable higher degrees of security without compromising aesthetics, customer service, user-friendliness, or overall hospitality. Access control can protect critical areas such as pharmacies, surgery room, infant treatment rooms, technology closets/rooms, information storage rooms, and areas that separate staff from the public.

Protection is important to every healthcare administrator, but so is properly managing the first view patients and visitors have of the facility. This means that access control systems used should not display a predominance of unfriendly barriers or obstructions.

A defined philosophy of “onstage” and “offstage” is an important consideration in the design. Defining and separating out areas that are open to the public and those that are not are important first steps. Once closed areas are identified, determining the level of security access and how restricted it should be follows.

After hours continues to be the primary time of security risk in healthcare facilities. Having a single clearance point to areas such as the emergency department or other single designated point of entry is recommended to control access into the facility after normal business hours.

One of the most fundamental concerns within a healthcare facility is the ability to manage properly and swiftly serious emergencies. Frequently, this requires the ability to restrict access into the facility as a whole. Lockdown procedures dominate discussions relating to emergency preparedness for healthcare organizations. How fast the healthcare facility can be locked down is a key indicator for facility readiness to many internal and external disasters, riots, civil disturbances, and other workplace violence scenarios.

In short, a sophisticated, electronic access control system is one of the most cost-effective security investments a healthcare facility can make.

## Where Are Alarms Needed?

The two basic security alarm applications found in healthcare facilities are the intrusion alarm and the duress alarm. Simple intrusion detection is probably the most familiar concept of security technology. Intrusion detection involves the use of door or window contacts, glass contacts, and motion sensors in combination with some type of audible alarm that sounds when a person has forced entry into a building or room. An alert is sent to a central security station to notify the security department, or authorities, of the time and location of the alarm activation.

The intrusion alarm is used for sensitive areas within a healthcare facility that are closed for certain periods, including clinics, pharmacies, laundries, general stores, medical records, libraries, and gift shops. The intrusion alarm is also a primary safeguard utilized for satellite pharmacies, offsite facilities, and medical office buildings.

The duress alarm is frequently used in cashier’s offices, pharmacies, and gift shops. This type of alarm is more often used to summon security personnel to observe suspicious people or activities rather than solely as a holdup alarm. Duress alarms are used in behavioral health units, emergency departments, and remote work locations to summon both security officers and/or medical assistance.

## Why Invest in Video Surveillance?

Video surveillance systems [or closed-circuit television (CCTV)] have evolved significantly in the past several years. General surveillance is one of the basic uses of CCTV. When used for this purpose, the system is perhaps more of a psychological deterrence than an actual physical control.



Video surveillance, access control, and alarms have much in common, and they often work together as an integrated system to keep intruders out of secure areas, limit access to security-sensitive areas, and remotely monitor critical areas to reduce the risk of crime and security incidents. It is why more and more healthcare organizations continue to increase their use of video surveillance as part of their overall security plan. Integrated together, the technologies help to render security personnel more effective.

Properly located video surveillance cameras can extend the range of the security staff and provide valuable incident information. Studies have found that video surveillance can have a significant deterrent effect on property crime but it will not, however, deter all crime. The use of recorded video images has resulted in countless arrests when shared with law enforcement authorities or when appropriately released to media outlets. In no situation should dummy, or nonoperating, cameras be used.

The most important consideration in a video surveillance system is the quality of the image received, and this is largely dependent on the camera and recording equipment used. As a general rule, all cameras utilized in a security system for after-the-fact investigation and overall deterrence should be recorded and the recording retained in a 10-day library at a minimum. It is not uncommon to maintain recorded images for 30 days. Common exceptions to this rule are video surveillance systems used in patient care areas or for patient monitoring.

Healthcare organizations that authorize video monitoring of patients typically require the video to be watched at all times. The recording of the video monitoring should be kept in a secure location, used only for the purpose for which it was recorded, and not be released, used, or disclosed to others. The driving purpose for the use and application of the video surveillance should govern whether or not it is recorded. For future protection, the purpose and use of each camera should be documented in the security master plan.

Should video surveillance systems be constantly viewed is a commonly asked question. The answer depends on the application. Many video surveillance systems are integrated into the protection system and designed to only capture (record) images to be utilized later, if necessary. In these systems, there may or may not be any live monitoring involved. Live monitoring is rarely a cost-effective use of resource as a security officer can generally view a monitor for only 30 minutes or less without becoming bored or ineffective. If live monitoring is required, event-driven monitoring is a better alternative. This monitoring equipment alerts the operator when the monitor must be viewed. In these systems, the monitor to be viewed will often be automatically shifted to a larger screen and will activate recording equipment.

## What Other Security Technology Applications Should Be Considered?

There are numerous security technologies used in the healthcare environment to protect people, safeguard assets, and protect the reputation of the organizations. These include radio communications, visitor management systems, emergency call boxes, mass notification, asset tracking, and metal screening.

### *Radio Communication*

The most important piece of equipment a security officer can carry is the two-way radio, which is part of the overall security communications system. A one-way pager is simply unacceptable. Not only does the radio provide an element of personal safety for the officer, but it is essential in achieving an effective security system.

Good communications equipment is expensive; however, the cost has been reduced in recent years. Considering the life of today's equipment, the cost, depreciated over the number of usable years, is the best investment of security dollars that an organization can make.

### *Visitor Management*

Visitor management systems are not new to the healthcare industry as patient rosters and paper guest logs have been used at information desks to help with way-finding and guidance for years. What is new is the computerized way to capture detailed visitor information and to accurately identify, badge, and track visitors, vendors, and other authorized personnel entering the healthcare facility and the purpose of their visit. One of the greatest benefits of the more advanced visitor management systems is the ability to incorporate programmable security alerts or watch lists. The more sophisticated systems can check each visitor's name against a list of people who should not be allowed to enter the building (former employees, estranged spouses, etc.) and alerts the security officer or greeter when a match is found, telling him/her how to handle the situation.

The downside to the use visitor management systems is typically not cost-related or the advantages of the features offered, but the visitor queuing that can result in a processing backlog. Many healthcare administrators remain very concerned about the image presented in the main lobby and resist any system that obstructs or delays patient or visitor access to the facility during regular business hours. However, most of these same administrators desire to more strictly manage visitation to the organization after normal business hours or at the end of specified visiting hours.

### *Emergency Call Boxes*

*Emergency phones, call boxes, phone towers, or wall-mounted emergency phones* are all names used to describe the emergency phone system designed to connect a potential victim of crime or someone in need of service with security. Strategically locating these free-standing devices or wall-mounted units in surface parking lots, garages, and other high-pedestrian-traffic areas on campus can help facilitate immediate assistance to those requesting it. Most emergency call telephones are equipped with a blue-light strobe on top of the device to enhance visibility. When flashing, it helps expedite security officer response and let others in the vicinity know that assistance is needed. An added benefit may be to scare off a person intent upon criminal or wrongdoing activity.

Emergency phone systems are also used for nonemergency purposes and can be excellent customer service tools for employees, staff, and visitors who may need basic assistance. These devices, when used, are excellent crime prevention and public

relations tools as they demonstrate a visible organizational commitment to a safe and secure environment.

### *Mass Notification*

The 2007 Virginia Tech University tragedy served as a wake-up call for many healthcare facilities and has yielded numerous lessons learned that has prompted many to reassess how they prepare for, respond to, and mitigate incidents of targeted violence. Specifically, this tragedy identified the need for the healthcare facility to have a quick and facility-/campus-wide notification of a threat or emergency. Technology advances have provided many mass notification solutions available to the healthcare facility. In many instances, the use of e-mails and pagers has supplanted overhead announcements; however, many healthcare organizations have realized that multiple modes of notification are needed to reach all of constituents inside the facility and the campus grounds.

### *Asset Tracking*

Many hospitals have started to protect their assets with wireless radio frequency identification technology (RFID), which uses small transmitters attached to the protected equipment that communicate with the organization's access control system. Similar to the unobtrusive security tags used on store merchandise to thwart shoplifters, RFID tags are often used to track equipment as it moves through various doors and can detect where a piece of equipment is located within the organization or if it leaves the facility. In short, an RFID tag can be attached to just about anything of value, such as an EKG monitor or mobile workstation, and can be easily tracked throughout the facility.

### *Metal Screening*

Philosophically, there are some healthcare environments that lend themselves to metal screening. The most likely application in a healthcare setting is the Emergency Department. The recommendation, introduction, and management of metal screening programs in healthcare cannot be done in a vacuum. The security improvements are considerable; however, the introduction of metal screening has employee relations and organizational culture implications in addition to patient and community perceptions that must be addressed collectively. The placement and exact location of the metal detector are important considerations. The device should be installed to minimize unnecessary delays in the queuing of patients and visitors and fit comfortably into the aesthetic décor of the facility. And of course, there are budget issues to be considered to include security officers to staff the device.

## **The Investment in Security Technology Has Been Made. How Do We Know It Works?**

Many electronic security systems are used to keep healthcare facilities safe. But one of the common missing components is the routine testing of these systems. Systems or

components are commonly found to be ineffective, not working as originally intended, and/or not meeting current needs—creating unnecessary risk and liability exposure for the healthcare organization.

The documentation and testing that should be required of every healthcare security program may be considered small and routine. However, their importance is found in the liability protection afforded to the facility and more prominently, the positive perception of security and the protection department.

## How Concerned Should We Be About Violence in Healthcare?

Workplace violence is an industry-wide healthcare problem and not exclusive to any one healthcare organization. Violence threatens the safety of staff, patients, and visitors in hospitals and healthcare organizations of all sizes and settings. It demoralizes healthcare professionals, especially nurses, who are most often the victims of violence, and costs hospitals untold millions in lost time, employee turnover, reputation for quality care, and additional security measures.

Regardless of the patient care services offered, the threat of violence in the workplace is all around us—no healing environment is immune from having violent acts occur inside the facility or on its campus. Approximately half of the nurses responding to a 2007 survey conducted by the Emergency Nurses Association believe that violence is simply part of their everyday work environment.<sup>4</sup> In the survey, 9 out of 10 Emergency Department Managers cited patient violence as the greatest threat to department personnel.

The majority of people generally associate violence in the workplace with assault and homicide, not with intimidating postures or expressions of mild anger. It is important that the healthcare administrator break workplace violence down into *actual* violence and the *threat* of violence. Both can create a hostile and uncomfortable work environment, and even with this breakdown, healthcare workers face significantly higher risk of injury from nonfatal assaults (actual violence) than that of other workers.

The clinical patient is often the source of confrontation, largely due to the volume of patients, long waits, and disputes relative to services being rendered. Hospital emergency departments, along with mental health evaluation and treatment areas, intensive care units, dedicated forensic patient care centers, and closed head injury units, have historically had the highest potential for violence. There are countless cases in which patients have attacked staff ostensibly without warning or provocation.

The problem of escalating violence is worsened by the restrictions imposed by regulatory and accreditation agencies such as CMS and TJC that require healthcare organizations to apply medical restraints or seclude patients as a means of last resort. The overly strict interpretations by surveyors and healthcare organizations alike have resulted in the compromise of employee, staff, and physician safety. Care providers are rarely using the tools available to them until after an actual incident of violence occurs. The result is more incidents of violence and more injuries to healthcare workers and patients alike. To correct this vicious cycle, TJC, CMS, and healthcare organizations must take a more balanced

approach in its interpretation of these patient restraint and seclusion guidelines before a safe and therapeutic healing environment can be created. If not, healthcare professionals will continue to leave healthcare occupations because of the risk of actual and threat of violence, increasing the industry-wide shortage of qualified medical professionals.

The patient is the primary but not the only source of workplace violence; employees and staff members have been the source of many violent acts. The day-to-day supervision, work evaluations, disciplinary actions, and terminations all set up situations that can be confrontational and that can provide the motivation of employee and ex-employee violence.

There is a potential for workplace violence caused by individuals or groups who are from outside the organization, which may include legitimate visitors such as patient family members or illegitimate visitors. The latter type of visitor includes criminals contemplating or committing a crime (robbery, abduction, assault); gang members intent upon causing injury or harm; unwelcome friends or family members of staff or patients; protestors; terrorists; transient persons; and former patients and employees. It is almost impossible to discern the presence and intent of these persons until an overt act occurs. They often blend in with the legitimate patient, staff, or visitor.

Not all violence occurring in the healthcare environment can be prevented; however, many acts can be prevented and managed to minimize injury, death, and damage to property. All organizations need a strategy and plan to deal with workplace violence so that they can reduce the number of violent incidents and minimize the severity of these incidents to a large extent.

There are three specific steps of preparation and response that organizations must implement to properly address workplace violence. The first step is to provide a reasonable level of security for the overall environment and especially to areas of probable conflict. This includes an organized security program that includes access control plans, proper physical security safeguards, enforced security policies and procedures, staff training, empowerment, and an effective critical incident response capability. To adequately plan and implement these essential elements, there must be a strong commitment from the top management, and the board of directors, to provide a high level of philosophical and management support. This support includes adequate funding of the protection program.

The second phase is an organizational threat policy. The foundation of a successful violence prevention program is that the policy should state clearly that threats of any kind are not tolerated and that the staff is responsible for reporting all threats, and what the procedures are for reporting such threats.

The third phase is a response plan that is based on recognizing, understanding, reacting to, and managing events as they develop and escalate. There should be a specific response team that evaluates and plans actions concerning all threats. The team should comprise the security administrator, director of human resources, nursing administrator, and in some cases the risk manager. The coordinator or leader of this team should initially decide the team member or combination of team members responsible for the

management of the threat. All threats must be taken seriously. The degree and severity of the threat will be somewhat of a subjective judgment in terms of actions to be taken. It is better to err on the side of taking too much action than doing too little too late.

Fundamental to any workplace violence prevention strategy is conflict resolution training. While there is no program that can train healthcare staff to handle every type of violent situation, most healthcare security administrators agree that it is possible to train them on the commonalities that occur in these situations. Most crisis intervention training programs include these lessons and help the employee look for physiological clues that an individual's aggressive behavior might escalate.

The cost of violence in healthcare settings is great. It affects the patients' recovery as well as causing physical and psychological injuries to staff. Victims can suffer physical and psychological pain, confidence can be irrevocably shaken, and stress levels debilitating. With the growing crisis over nurse shortages, it is all the more important that healthcare organizations send a message that violence against nurses and medical care providers in general will not be tolerated. Violence should not be an accepted part of the job for any medical care professional, security officer, or other employee in the healthcare environment. Many assaults in healthcare settings are premeditated and perpetrated by patients who have a history of violence that should be communicated to caregivers on admission. The healthcare organization should take a stand and hold perpetrators of these assaults accountable for their actions.

#### *Are We Doing Enough to Protect Our Infant and Pediatric Patients?*

Infant abduction prevention is a top concern for hospital administrators, and security of infants is certainly a priority, both for safety and public relations reasons. Statistically, the risk of an actual abduction is low. All told, 126 newborns have been abducted by strangers from hospitals since 1983.<sup>6</sup> However, statistical relevance is not important to the family that is the victim of abduction, the healthcare organization's staff, the healthcare facility, or the public. This event is devastating and takes an emotional and physical toll on all involved. The organization's reputation for safe patient care may suffer as well even if the organization does everything appropriate to avoid an abduction.

The areas of greatest risk for infant and child abductions include the mother's room, nursery, post partum units, pediatric care areas, and neonatal intensive care units as well as well-baby units. But because these units may present more of a challenge to anyone trying to abduct an infant, an abductor may try to abduct a child in waiting areas for hospital clinics, radiology, and the emergency department.

The basics of providing infant security are identification (mom, baby, significant other, and the caregiver staff), education (mom and staff), and physical and electronic security safeguards. Video surveillance and controlling access to prevent unauthorized visitors from gaining access to the mother/baby unit must work collectively together and in conjunction with staff training, parental education, and a critical incident response plan that is frequently tested and exercised.

There has been a good deal of interest by healthcare security organizations in the electronic monitoring of infants. Infant tagging is useful in preventing newborn abductions, but it is not foolproof. Cathy Nahirny, Administrative Manager with the National Center for Missing and Exploited Children, has documented 14 cases where an infant was abducted by a nonfamily member from a healthcare facility and the facility had installed an infant security tagging system.<sup>7</sup> These infant-tagging systems cost anywhere from several thousand dollars for a single door alarm to several hundred thousand dollars for a very sophisticated system. However, the decision to install any electronic monitoring system should not be based on funding alone. There must be a complete buy-in by unit staff, as these systems require human involvement to make them effective. If used, the infant tagging system should be integrated with door and elevator controls and video surveillance systems to accentuate the protection of infants and harden the organization as a target for a potential abductor.

#### *What Should We Do Differently to Manage Forensic Patients?*

The forensic patient continues to be both an issue and challenge for healthcare administrators. The forensic patient may either be brought to the medical care facility for emergency or outpatient treatment or for a planned hospitalization as an inpatient. In all cases, the forensic patient must be viewed as a potential threat to the facility. The typical healthcare facility does not host an environment that is well equipped or prepared for management of forensic patients, but at any given point in time, there may be prisoners inside a healthcare facility.

Confusion and conflict can take place when caring for the forensic patient. Law enforcement or correctional personnel often do not understand the procedures of medical care, while medical care staff do not always understand the implications of the custody of the patient. It is important that the prisoner remain in the custody of the correctional officer at all times to include being properly shackled to the wheelchair or gurney. Medical care staff should never ask to remove restraints unless medically required. In such instances, an alternative restraint should always be added to include temporary use of medical-restraint devices. If this is not possible, the healthcare organization should require more than one correctional officer to assist in managing unrestrained forensic patients. Managing unrestrained prisoners alone in any environment is inherently dangerous and should not be tolerated.

#### **How Do We Get Employee Involvement in the Protection Effort?**

It is universally agreed among security administrators that staff must take ownership in directly contributing to the protection of the organization; however, there are issues beyond practicing good security. A primary function of any protection system is to educate, stimulate, and motivate the first-line protection resource: employees. The protection level of a medical care facility is directly related to the extent to which employees participate in the security effort.

Employee education begins with new employee orientation. New employees can be channeled into the protection system with a minimum of effort. They seek the norms and want to know what their employer expects. The moment employees first enter the workplace is the prime time to develop a positive protection attitude. Employees will not remember everything that is presented, but they will form a basic opinion, either consciously or unconsciously, of the importance that the organization places on security. Crime prevention presentations, handouts, events, and training can also raise staff awareness of security issues. Not only will this add eyes and ears to the security effort, it will be noted by TJC surveyors and other regulatory agencies, which are increasingly looking for employee involvement in the healthcare security program.

Various functions of the healthcare security program must work together to reduce security risks and provide tangible benefits in support of the organizational mission. Each organization must determine how the functional security program elements will be implemented and managed. They may be assigned to different individuals and departments, or they may be brought together under a specific department or division. In this respect not all elements of a protection system are performed by one department.

One of these issues is the authority for intervention. When security is called to a nursing unit because a patient or visitor is out of control, who is responsible for directing actions—security or nursing? The answer is either one may be appropriate; however, this role should be clear in the strategic plan and protection of the resultant policy/procedure. When there are drugs missing from the pharmacy, is this a pharmacy problem with support from security or a security problem to be resolved by security with support from the pharmacy? When a laptop computer belonging to the organization is stolen, can the employee simply order another one, or does it require a report to security before the purchasing unit will order or otherwise provide a new one? These are the types of strategic questions that must be answered from a strategic context to provide the proper operating fabric and coordinated direction of the protection effort.

## What Security-Related Policy and Procedures Do I Need?

A basic component of the successful security program is a comprehensive and useful documentation system. Records and reports maintain a large majority of the security program documentation to fulfill various administrative needs and verify security activity. These reports are important for general department planning purposes, the capture of findings from incident activity and follow-up investigative activity, and often legal consequences in the advent of an adverse security event. The retention of security operational records should be controlled by organization policy, subject to any state law, that ensures that needed records are retained and unneeded records are discarded or destroyed as necessary.

A major function of the protection system is to manage employee actions and response to adverse events that protect the organization's well-being and the personal safety of all constituents working at, visiting, or receiving patient care services from the healthcare facility. This is most frequently accomplished with organizational policy and procedures. [Table 25-4](#) provides a comprehensive list of security-related policy and procedures that



**Table 25-4** Security-Related Policy and Procedures

Security-Related Policy and Procedures	
Active Shooter	Access Control: After Hours, Facility-Wide, Restricted Access (lockdown), Security Sensitive Areas
Armed Robbery and Response	Bomb Threat
Calling for Police Response	Confiscation of Prohibited Items
Employee Drug Testing	Employee Security Education
Employee Security Responsibility	Forensic (Prisoner) Patients
Gang Behavior: Recognizing and Responding	Hostage Situation
Infant and Pediatric Abduction Prevention and Response	Identification: Employees, Visitors, Vendors
Law Enforcement Requests for Information about Patients	Package Inspection
Parking Control and Violation	Patient Elopement Prevention and Response
Patient Search	Patient Valuables
Preemployment and Ongoing Background Check	Public Safety Liaison
Management of the Combative Patient	Missing Patients
Munchausen by Proxy Syndrome	Security Involvement in Patient Assistance
Security Sensitive Area Access Control and Critical Incident Response Plans	Weapons and Contraband Prohibited
Workplace Violence Prevention and Response	Very Important Patients

every healthcare administrator should require to be evaluated for appropriateness to their environment.

### What Performance Metrics Should I Be Using for Benchmarking My Security Program?

On an annual basis there should be a formal review of the security program which addresses the objectives, scope, performance, and effectiveness of both the security management plan and the operational implementation of the plan. In short, how did the program measure up to expectations? In addition to the security management plan the periodic reports prepared throughout the year for the multidisciplinary review committee are the basic sources of information for the annual evaluation. The annual evaluation does not need to be on a calendar year basis; however, the calendar year is utilized by most healthcare security administrators. The annual security program effectiveness evaluation continues to be a requirement of TJC.

The setting of security goals and the evaluation of the success in meeting those goals is an important stimulus for attentive action by the security staff. If you cannot measure

the performance of your security program, you will never know if expenditures were a wise investment. There are other measures of performance. What is the security department's reputation among the stakeholders and outside agencies that security interacts with. Although not a metric, the healthcare executive who moves about the facility and really listens will basically know how good (or bad) the security program is functioning.

## References

1. Taxin, A. (2009, April 16). Police: 3 dead in California hospital shooting. *The Associated Press*. Retrieved April 22, 2009 from <http://www.foxnews.com/story/0,2933,516888,00.html>.
2. Rivard, R. (2009, June 16). Many hospitals seeing increase in violence. *Charleston Daily Mail*. Retrieved June 16, 2009 from <http://www.dailymail.com/News/200906150690>.
3. Associated Press (2009, July 20). Man shoots ex-girlfriend, self at Texas hospital. *Foxnews.com*. Retrieved July 21, 2009 from <http://www.foxnews.com/story/0,2933,534113,00.html>.
4. Emergency Nurses Association. (2007). *Study of workplace violence against registered nurses in emergency departments*. Retrieved June 8, 2008 from <http://www.ena.org/research/current>.
5. Weronik, R. (2008, January 21). *Securing our hospitals: GE security and IAHS healthcare benchmarking study*. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar.
6. Raburn, J., Jr., & Nahirny, C. (2009, March 24). Newborn/infant abductions. *National Center for Missing and Exploited Children*.
7. Nahirny, C., & Ryce, J. (2009, March 27). Infants abducted from hospitals with security tagging systems. *National Center for Missing and Exploited Children*.



# Glossary

**Access Control** The control of persons, vehicles, and materials through entrances and exits of a protected area; an aspect of security that often utilizes hardware systems and specialized procedures to control and monitor movements into, out of, or within a protected area. Access to various areas may be limited to place or time, or a combination of both.

**Accreditation Watch** An attribute of an organization's Joint Commission accreditation status; a health care organization is placed on Accreditation Watch when a reviewable sentinel event has occurred and has come to the Joint Commission's attention, and a thorough and credible root cause analysis of the sentinel event and action plan have not been completed within a specified time frame.

**Active Shooter** An armed person who has used deadly physical force on other persons and continues to do so while having unrestricted access to additional victims; active shooters have caused a paradigm shift in law enforcement and security training and tactics, especially as these persons do not necessarily expect to escape or even survive these situations.

**Acts of Violence** Any physical action, whether intentional or reckless, that harms or threatens the safety of another individual in the workplace.

**Acquired Immunodeficiency Syndrome (AIDS)** A disease of the body's immune system caused by the human immunodeficiency virus (HIV). AIDS is characterized by the death of CD4 cells (an important part of the body's immune system), which leaves the body vulnerable to life-threatening conditions such as infections and cancers.

**ANSI** American National Standards Institute

**Asphyxia** A lack of oxygen or excess of carbon dioxide in the body that is usually caused by interruption of breathing and results in unconsciousness.

**At-Risk Patient** A patient who is or has:

- Been placed on a mental-health or alcohol hold in accordance with Colorado law,
- Acute Drug/ETOH intoxication,
- Head-injured with altered mental status,
- Confused to time, place, and/or person,

- At Risk for elopement based on past history or current condition,
- Disruptive or violent (patient may lose control, threaten to lose control, or give others evidence of a deteriorating mental condition),
- Indication(s) of a weapon or other dangerous item.

**Audit** An examination of procedures and practices conducted for the purpose of identifying and correcting unwanted conditions.

**Bullet-Resistant Glazing** Glass consisting of two or more plates bonded with plastic (polycarbonate material) interlays.

**Center for Medicare and Medicaid Services (CMS)** The agency in the US Department of Health and Human Services responsible for administering the Medicaid, Medicare, and State Children's Health Insurance programs at the federal level.

**Change Key** A key to a single lock within a master key control system.

**Closed-Circuit Television (CCTV)** A video surveillance system; a television installation in which the signal is transmitted to a defined number of receivers.

**CN Agent** The descriptor for chloroacetophenone, a riot-control chemical agent that causes severe weeping or tearing of the eyes. CN is a commonly used tear gas that produces a characteristic apple blossom odor and is released as a particulate cloud, or dissolved and released as a liquid aerosol. Within seconds after exposure to it, CN irritates the upper respiratory system and eyes, causing tears. In heavy concentrations, this agent is irritating to the skin and can cause a burning, itching sensation on moist parts of the body.

**Collapsible Baton** A weapon occasionally used by security officers to maintain control. It has the advantage of being expandable and durable to not collapse when in use; can be collapsed down to a smaller size for carrying ease. Also referred to as an expandable baton.

**Color Rendering Index** The effect of a specific light source on the color appearance of objects.

**Common Law** Also known as Case Law and distinguished from an Act of the legislature. Includes all judgments and decrees of the Court interpreting and applying acts of the legislature and recognizing common custom and usage, especially the ancient unwritten law of England.

**Community Hospitals** A short-stay general or specialty (e.g., women's, children's, eye, orthopedic) hospital, excluding those owned by the federal government.

**Competency** The quality of being adequately or well qualified physically and intellectually.

**Convergence** The merging of physical security safeguards and information technology to provide a coordinated organization risk management system.

**Covert** The observation of someone by another person or equipment which is hidden from view, usually to detect suspicious or illegal activity.

**CPTED** Crime Prevention Through Environmental Design

**Crime Prevention** A pattern of attitudes and behaviors directed both at reducing the threat of crime and enhancing the sense of safety and security, to positively influence the quality of life in our society, and to help develop environments where crime cannot flourish.

**Crime Triangle** The three basic elements necessary for a crime to occur: a criminal with the desire and ability to commit a crime, and a victim who provides an opportunity for the crime.

**Critical Access Hospital** A hospital with a patient census of less than 25, located more than 35 miles from a hospital or another critical access hospital, or certified by the state as being a necessary provider of health care services to residents in the area.

**Critical Incident Response** Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as to provide services to the surviving population. Response steps should include potential crisis recognition, notification, situation assessment, and crisis declaration, plan execution, communications, and resource management.

**Critical Incident Response Plan** Unit employee response to the primary security threat of a security sensitive area including how employees respond to predetermined events that negatively impact department performance and/or personal security (usually those events which caused the area to be declared security sensitive).

**Defamation** Includes both Libel (the written word you can “L”ook at) and Slander (the “S”poken word). Communication which is false and tends to injure the reputation of another. Untrue communication, which ridicules another. Instead, always cite/name your source. “Quote” their statement when appropriate in your report. Never share confidential information outside the department.

**Digital Video Recorders (DVRs)** Developed to replace video tape recorders; a video storage device that takes an analog signal and processes, compresses, and stores the image in a library of files in which search and perform queries can be performed.

**Discipline** Making yourself do something regularly: to make yourself act or work in a controlled or systematic way.

**Discrimination** Treatment of another that is not consistent with others whether with regard to disciplinary action or rewards.

**Drug Diversion** The redirection of legally manufactured controlled drugs, substances, and implements (paraphernalia) for the introduction of drugs into the illegal market. Drug diversion occurs within the legitimate system for distributing drugs through wholesalers, retailers, hospitals, clinics, research agencies, doctors, and nurses.

**Dummy Camera** A genuine-appearing but nonfunctional camera used as a crime deterrent. It is typically mounted out of reach in a conspicuous spot at a place having a history of employee pilferage, shoplifting, misconduct, robbery, etc. Some models are stationary, some scan, and most are equipped with a red pilot lamp. Also called as simulated camera.

**Duress Alarm** A device that enables a person under duress to call for help without arousing suspicion.

**Duress Code** A special code that reports an ambush, duress, or emergency situation. The code can be given verbally, for example, as part of what would appear to be routine conversation, or entered on a digital keyboard during what would appear to be a routine disarming sequence or call-in.

**Duty Belt** Typically constructed of nylon or leather, a belt designed for security officers to carry equipment easily, in a readily-accessible manner, while leaving the hands free to interact.

**Duty of Care** Employers have a duty to exercise reasonable care in hiring individuals who, because of the type of employment and amount of contact with the public, may pose a threat of injury to members of the public.

**Electromagnetic Interference (EMI)** The disruption of operation of an electronic device when it is in the vicinity of an electromagnetic field (EM field) in the radio frequency (RF) spectrum that is caused by another electronic device.

**Electronic Control Devices (ECD)** Use propelled wires or direct contact to conduct energy to affect the sensory and motor functions of the nervous system.

**Emergency Medical Treatment and Active Labor Act** EMTALA is legislation that originated as a part of COBRA to prevent hospitals from refusing to see patients who come to the emergency room based on insurance or uninsurance status. EMTALA requires that all Medicare participating hospitals screen and stabilize all individuals coming to an emergency room and all individuals coming to a hospital seeking emergency medical services. EMTALA imposes fines and possible exclusion from the Medicare program for violations.

**Emergency Operations Plan** Hospital and health care providers may have the emergent need to isolate large numbers of patients/victims due to infectious disease outbreaks or chemical, biological, radiological, or nuclear events. To meet this need, specialized planning,

organization, and protection of employees is required. This Emergency Operations Plan should describe the development and operation of a unit to accommodate such a need.

**Emotional Intelligence** How leaders handle themselves and their relationships.

**Enterprise Risk Management** The emerging discipline that integrates traditional security with information technology to produce a holistic perspective in managing organizational risks.

**Fixed-Post Assignment** The fixed-post assignment is the most restrictive of all deployment methods. The individual assigned to a fixed post generally has no discretionary autonomy in terms of geographical location and generally cannot leave the post unless relieved by another individual.

**Foot Candle (FC)** A unit for measuring the intensity of illumination; the amount of light a single candle provides over a square foot.

**Forensic Patient** A prisoner patient seeking medical attention or care in a health care facility under the custody of a law-enforcement or corrections agency.

**Full Time Equivalent (FTE)** A unit of measurement related to employee(s) working the equivalent of 40 hours per week, two individuals each working 20 hours per week, three individuals each working 13.33, etc. In some cases, an organization will consider a person working 32, 34, or 36 hours as full time for benefits purposes; however, those numbers are seldom utilized to calculate the number of FTEs. The FTE number is commonly utilized for budget purposes and does not indicate the number of persons employed (that is, the number of full-time versus part-time or contingent employees).

**Glazing** Transparent or translucent material used in windows, walls, and doors to admit light.

**Grand Master Key** A key that will operate two or more master key groups.

**Hacker** The name originally given to a person who took pleasure by learning the details of programming systems in a nondestructive manner; when such activities become destructive, the term becomes cracker; i.e., someone who cracks or cracks into a protected computer system.

**Hazard Vulnerability Analysis** A process used by health care facilities to identify potential emergency events that have the potential to impact the ability to meet a demand for services.

**Healthcare Provider** An individual or entity licensed or otherwise authorized under state law to provide health care services, such as doctors, hospitals, and nurses.

**Health Insurance Portability and Accountability Act (HIPAA)** Although HIPAA is applicable to the health care industry generally, HIPAA's Administrative Simplification

provisions and Health Insurance Portability provisions are particularly relevant for state Medicaid programs.

**Health Maintenance Organizations (HMO)** A form of health insurance that emphasizes comprehensive care under a single insurance premium; it is designed to eliminate unnecessary costs and to improve quality and acceptability of service through sharing the risk for the cost of care.

**Hospital Incident Command System (HICS)** Developed by California's Emergency Medical Services Authority; the HICS model intended to be used by all hospitals, regardless of their size or patient care capabilities, and to assist with their emergency planning and response efforts for all hazards. By embracing the concepts and incident command design outlined in HICS, a hospital is positioned to be consistent with National Incident Management System (NIMS) incident command design guidelines and to participate in a system that promotes greater national standardization in terminology, response concepts, and procedures.

**Human Immunodeficiency Virus (HIV)** The virus that causes AIDS. HIV is in the retrovirus family, and two types have been identified: HIV-1 and HIV-2. HIV-1 is responsible for most HIV infections throughout the world, while HIV-2 is found primarily in West Africa.

**Inadequate Security** Security measures that were provided to safeguard employees, customers, and members of the public, not consistent with the potential threat.

**Incident Command System (ICS)** A standardized response management system that is a key component of the NIMS. It is an "all hazard/all risk" approach to managing crisis and noncrisis response operations by enhancing command, control, and communication capabilities. Joint private/public sector planning establishes a smooth transfer of authority from the private sector to the public sector Incident Commander when he arrives on the scene. Unified command may occur after this transfer.

**Integration** A system to allow different physical security components to work together in a coordinated (integrated) approach of mutual support.

**Interim Management** The temporary provision of day-to-day direction and control of departmental operations by either an acting organizational employee or an out-sourced individual.

**Internal Control** A plan of organization and all of the methods and measures adopted within a business to safeguard its assets, check the reliability and accuracy of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies.

**Invasion of Privacy** The making public of facts to which one has a legally enforceable expectation of privacy. Unlike defamation, truth is not an available defense in a privacy



action. Eavesdropping, making public security department or patient records, wire taps, surreptitious audio or video surveillance may constitute invasion of privacy depending on applicable state and federal law.

**IP Cameras** Networked digital video camera that transmits data over a Fast Ethernet link. Commonly called “network cameras,” a digitized and networked version of CCTV.

**Job Task Analysis** The process of identifying and determining in detail the particular duties and requirements and the relative importance of these duties for a given job.

**Knox-Box** Known officially as the *KNOX-BOX Rapid Entry System*, it is a small wall-mounted box that holds building keys for firefighters and EMTs to retrieve in case of the need for an emergency entry.

**Learning Management Software (LMS)** Facilitates the delivery of technology-enabled training.

**Leaving Against Medical Advice (AMA)** Patient who presents to the facility for clinical evaluation, leaves before necessary steps for assessment and treatment are completed, and was informed of the risks of leaving.

**Line Inspection** The review of actions of individuals by a supervisor having direct control over those individuals.

**Lock** Any device or piece of equipment, which prevents access or use by requiring special knowledge or equipment.

**Magnetic Lock** A door lock consisting of an electromagnet and strike plate. The electromagnet is mounted in the doorframe opposite the strike plate, which is mounted in the door. When current is applied, the strength of the magnet holds the door locked. Magnetic locks operate on low voltage and consume little power.

**Magnetic Stripe Card** A plastic card with a data-encoded stripe on one face.

**Magnetometer** A sensor that operates by creating a balanced magnetic field between transmitting and receiving coils. The movement of a sufficient volume of metal through the field causes an imbalance, which triggers an alarm.

**Managed Care** Collective label for a broad range of changes in the financing mechanism for health care that transfer the costs back to providers, such as doctors and hospitals, and to users, patients, and their families.

**Master Key** A key, which will operate two or more sub-master lock configurations.

**Medicaid** Governmental assistance for care of the poor and, occasionally, the near-poor established through the state/federal program included in Public Law 89-97, Title 19.

**Medical Restraint** A subset of general physical restraint used for medical purposes. Unlike some other forms of restraint, medical restraints are designed to restrain their wearer without causing pain; generally used to prevent people with severe physical or mental disorders from harming themselves or others. A major goal of most medical restraints is to prevent injuries due to falls. Other medical restraints are intended to prevent a harmful behavior, such as hitting people.

**Medicare** It is the means-tested health care program for low-income Americans, administered by CMS in partnership with the States.

**Megapixel Cameras** A high-definition or extremely high-resolution camera; can only be used with IP systems.

**Miranda Rights** Legal rights during police questioning; the rights of a person being arrested to remain silent in order to avoid self-incrimination, and to have an attorney present during questioning.

**Missing Patient** A patient missing from a care area without staff knowledge or permission.

**Modified Fixed-Post Assignment** In this deployment assignment, the officer is mandated to be in a rather close geographical area, such as an emergency department, lobby, or staff entrance. The person may or may not be available to answer calls for service depending on the individual program directives.

**Motion Detection** Detection of an intruder by making use of the change in location or orientation in a protected area as the intruder moves around. In video motion detection, this means changes in key parameters of a viewed scene from a recorded reference image of that scene.

**National Center for Missing and Exploited Children (NCMEC)** Established in 1984 as a private, nonprofit 501(c)(3) organization to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional mandates, the NCMEC:

- Serves as a clearinghouse of information about missing and exploited children.
- Operates a CyberTipline for the public to report Internet-related child sexual exploitation.
- Provides technical assistance in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children including publishing the *For Health care Professionals: Guidelines on Prevention of and Response to Infant Abductions*. Offers training programs to law-enforcement and social-service professionals.
- Distributes photographs and descriptions of missing children worldwide.
- Coordinates child-protection efforts with the private sector.
- Networks with nonprofit service providers and state clearinghouses about missing-persons cases.

Provides information about effective state legislation to help ensure the protection of children.

**National Incident Management System (NIMS)** The NIMS establishes standard incident management processes, protocols, and procedures so that all responders can work together more effectively. NIMS components include:

- Command and Management;
- Preparedness;
- Resource Management;
- Communications and Information Management;
- Supporting Technologies; and
- Ongoing Management and Maintenance.

**Negligence** The doing of that thing which a reasonably prudent person would not have done, or the failure to do that thing which a reasonably prudent person would have done in like or similar circumstances. It is the failure to exercise that degree of care and prudence that reasonably prudent persons would have exercised in similar circumstances.

**Negligent Hiring** The failure to properly screen employees, resulting in the hiring of someone that has a history of violent or criminal acts.

**Negligent Retention** Retaining an employee after the employer became aware of the employee's unsuitability, thereby failing to act on that knowledge.

**Negligent Supervision** Failing to provide the necessary monitoring to ensure that employees perform their duties properly.

**Network Video Recorders (NVRs)** Takes the video stream directly from the IP camera and archives it into a video library; almost identical to DVRs except they cannot capture analog video.

**Observation Room** This is a room within the emergency department medical treatment area used to administer care to the combative or "at-risk" patient.

**Oleoresin Capsicum (OC)** A naturally occurring substance found in the oily resin of cayenne and other varieties of peppers. It is used in pepper spray to incapacitate violence of threatening individuals.

**OSI** International Organization for Standards

**Patient- and Family-Centered Care** An innovative approach to the planning, delivery, and evaluation of health care that is ground in mutually beneficial partnerships among health care patients, families, and providers.

**Patient Elopement** Patient incapable of adequately protecting himself or herself, and who departs the health care facility without the knowledge and agreement of the clinical staff; also referred to as "absconding."

**Patient Search** An inspection of a patient and belongings by hospital or security staff.

**Personal Protective Equipment (PPE)** Used to reduce employee exposure to hazards when engineering and administrative controls are not feasible or effective in reducing these exposures to acceptable levels. The Occupational Safety & Health Administration (OSHA) requires employers to determine if PPE should be used to protect their workers.

**Physical Restraint** Any manual method or physical or mechanical device that restricts freedom of movement or normal access to one's body, material, or equipment, attached or adjacent to the patient's body that he or she cannot easily remove. Holding a patient in a manner that restricts his/her movement (this would include therapeutic holds) constitutes restraint for that patient.

**Plan-Do-Study-Act (PDSA) Cycle** A four-part method for discovering and correcting assignable causes to improve the quality of processes.

**Protective Vests** Protective covering worn by security officers that are designed to guard individuals in combat and withstand gunfire, sharp objects such as knives, or shrapnel; usually made of special materials such as Kevlar, Supplex, or CoolMax. Also called bulletproof vests.

**Proximity Card** Generic name for contactless integrated circuit devices used for security access and tracking systems.

**Radio Frequency Identification (RFID)** The electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum used to transmit signals. An RFID system consists of an antenna and a transceiver, which reads the RF and transfers the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted; an emerging technology that enables companies to better track assets, tools, and inventory.

**Risk Assessment** The process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

**Safe Room** A designated room within the emergency department medical treatment area that can be locked from the inside, as a place for staff, patients, and even visitors to "hide" due to an immediate threat of danger.

**Safety Net Hospitals** Provider organizations with a mandate or mission to deliver large amounts of care to uninsured and other vulnerable patients. Examples include community health centers, clinics, public hospitals, and some teaching hospitals.

**Schedule II–V Drugs** Pharmaceutical-controlled substances that have legitimate medical purpose and also have potential for abuse and psychological or physical dependence.

**Search Coordinator** The supervisor/charge nurse of the unit in which a patient is determined missing. This person immediately initiates and coordinates the search to locate the patient, until such time as this responsibility may be transferred to administration or an incident command center.

**Sectored or Zone-Post Assignment** In this type of deployment, persons are assigned a specific geographical area of patrol and are generally dispatched to calls for service. These persons may also be dispatched out of their zone to provide back up and support to another zone officer. A specific health care facility may have a different number of zones for different hours of the day.

**Security Incident** A security-related occurrence or action likely to lead to death, injury, or monetary loss. An assault against an employee, customer, or supplier on company property would be one example of a security incident.

**Security Risk** The potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.

**Security Sensitive Area** A location whose function or activity presents an environment in which there is a significant potential for injury, abduction, or security loss that would most likely severely impact the ability of the organization rendering a high quality of patient care.

**Security Vulnerability** An exploitable security weakness.

**Security Watch** The utilization of a security officer to prevent the patient from harming themselves and/or staff and/or to deter a patient elopement.

**Self-Awareness** Awareness of the full range of your feelings, both positive and negative.

**Self-Management** Ability to use awareness of your emotions to actively choose what you say and do.

**Sentinel Event** An unexpected occurrence involving death or serious physical or psychological injury, or the risk thereof. The phrase “or the risk thereof” includes any process variation for which a recurrence would carry a significant chance of a serious adverse outcome.

**Sexual Harassment** “Settled law” is any direct or “implied” request for sexual favors, which may result in preferential treatment. “Emerging law” is any sexually “hostile environment” “allowed to exist” whether or not directly engaged in or encouraged by a supervisor.

**Social Awareness** Being attuned to how others feel in the moment, lets a leader sense, say, and do what is appropriate; also defined as the ability empathize.

**Special Police Authority** Legal authority (police powers) granted to an individual with certain restrictions. This authority is generally granted in relation to specific job performance and while so engaged upon the property of the employer or in the performance of a specific function.

**Staff Inspection** The review of function, procedures, policy, and outcomes of specified program components.

**Stakeholder** One who has a share or an interest in the functionality of a particular enterprise, or affect the success of the organization.

**Standard of Care** The degree of care, which should be exercised under a particular set of circumstances. The standard required may be found at law or under a reasonably prudent, ordinary person test.

**Targeted Violence** A situation where an individual, individuals, or group are identified at risk of violence, usually from another specific individual such as in cases involving domestic violence. Often the perpetrator and target are known prior to an incident.

**The Joint Commission (TJC)** A national organization of representatives of health care providers, including American College of Physicians, American College of Surgeons, American Hospital Association, and American Medical Association, and consumer representatives. TJC offers inspection and accreditation on quality of operations to hospitals, home care agencies, long-term care facilities, and integrated health systems.

- *Administrative Simplification Provisions* Require State Medicaid programs to: (a) use standard code sets and identifiers for electronic transactions relating to the processing of health claims, (b) implement protocols and other system-wide techniques to adequately protect individual health information, and (c) apply technical and physical safeguards to prevent unauthorized access to health information.
- *Health Insurance Portability Provision* Prohibits group health plans from denying coverage to individuals with pre-existing conditions, when the individual had “creditable” coverage for at least 12 months and no lapse of 63 days or more. As this “creditable” coverage includes Medicaid, state Medicaid programs should ensure their systems are capable of assisting individuals to qualify for these protections in the event individuals are eligible for private insurance after enrollment in Medicaid.

**Threat of Violence** Any behavior that by its very nature could be interpreted by a reasonable person as an intent to cause physical harm to another individual.

**Training** An educational process by which teams and employees are made qualified and proficient about their roles and responsibilities.

**Trauma Care** Hospitals may be certified and designated as meeting criteria for trauma care levels by the American College of Surgeons (ACS). There are four levels of trauma care based on the size of the population served and the range of services provided.

1. Level I: Level I trauma centers serve large cities or densely populated areas, and are generally the lead hospital of a trauma care system. They provide leadership and care for every aspect of injury, from education and prevention to outreach and rehabilitation.
2. Level II: Level II trauma centers are categorized into two distinct models. In the first model, in population-dense regions, the Level II facility supplements the activities of the Level I institution in a cooperative agreement designed to optimize area resources for injured patients. In the second model, in less population-dense areas where a Level I center may not exist, the Level II serves as the lead trauma facility for a geographic area. Patients with more complex injuries may have to be transferred to a Level I center depending on local resources.
3. Level III: Serves communities that do not have immediate access to a Level I or II institution. Level III trauma centers provide continuous general surgery coverage and the capability to manage the initial care of the majority of injured patients. Planning for care of injured patients in these hospitals requires transfer agreements and standardized treatment protocols.
4. Level IV: Level IV trauma facilities, usually in rural areas, provide initial evaluation and assessment of injured patients, as well as 24-hour emergency coverage by a physician. These facilities supplement trauma care within a larger network of hospitals, with most patients transferring to facilities with more resources dedicated to treating injured patients.

### **Types of Violence**

- Type I event (*criminal*)—the perpetrator has no legitimate relationship to the health care facility.
- Type II event (*patient*)—committed by someone who is the recipient of a service provided by the health care facility or the victim.
- Type III event (*employee*)—committed by someone who has an employment-related involvement at the health care facility, such as current or former staff members.
- Type IV event (*domestic*)—relates to interpersonal violence at the health care facility and includes spouses, lovers, relatives, and friends or other visitors who have a dispute involving an employee, patient, physician, or contractor.

### **Unusual Occurrence Report (sometimes referred to as an Unusual Incident Report)**

A common health care organization report generally used to record the circumstances of a negative occurrence involving the care of a patient.

**Vicarious Liability** Means an employer will be held responsible for certain actions of the employee. Also principal held to answer for acts of agent (also referred to as *Respondent Superior*).

**Video Analytics** A technology applied in software that examines the video camera's field of view for patterns of movement that match real-life events, such as falling, fence climbing, lurking, and trip-lines.

**Video Surveillance** A TV system in which signals are not publicly distributed but are monitored for security and other purposes; also commonly referred to as CCTV.

**Wandering Patient** A patient who aimlessly moves about within the building or grounds without appreciation for their personal safety; strays beyond the view or control of staff without the intent of leaving.

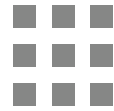
**Weapons of Mass Destruction (WMD)** Any destructive device that is intended or capable of causing death or serious injury to a large number of people through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors, disease-causing organisms, radiation or radioactivity, or conventional explosives sufficient for widespread lethality. See nuclear, biological, or chemical weapons (NBC).

**White-Collar Crime** A term relating to a wide variety of specific crimes committed for financial gain that are nonviolent and involve deceit, corruption, or breach of trust. Examples of such crime include fraud, bribes, kickbacks, computer-related crime, deceptive practices, illegal competition, tax evasion, fencing stolen property, and similar offenses.

**Workers Compensation** Cash benefits and medical care when a worker is injured in connection with work, and monetary payments to survivors in the case of death.

**Workplace Violence** A broad range of behaviors falling along a spectrum that, due to their nature and/or severity, significantly affect the workplace, generate a concern for personal safety, or result in physical injury or death.





# Appendix I

## Monthly Occurrence Report

For Period: 12/1/2009 to: 12/31/2009

Facility: **Sample Facility**

Total Incidents During Above Reporting Period at Sample Facility: 244

Category	Month Year	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.	Total
		2006	2006	2006	2006	2006	2006	2006	2006	2006	2006	2006	2006	
Alarm-Fire		10	5	8	3	3	8	6	9	3	3	10	6	74
Alarm-Security		30	21	15	45	41	42	40	39	68	59	66	80	546
Assault		2	1	0	0	2	1	4	0	2	1	2	0	15
Auto Accident		0	0	0	1	0	2	2	5	0	4	1	1	16
Burglary		0	0	0	0	0	0	0	0	0	0	1	0	1
Code Assistance		0	3	6	3	2	4	4	2	4	3	5	6	42
Disturbance		0	3	0	3	1	2	0	4	1	0	0	0	14
Drug Abuse		0	0	0	0	1	1	0	0	0	0	0	0	2
Found Property		0	0	0	1	1	0	0	0	0	0	0	0	2
Information Only		20	9	14	25	24	15	19	28	25	16	17	13	225
Missing Property		6	3	2	10	2	3	4	5	2	4	1	3	45
Patient Assistance		163	148	139	187	176	178	202	184	167	154	136	129	1963
Slip or Fall		1	1	1	0	0	0	0	1	2	2	0	1	9
Suspicious Person		5	8	7	10	9	15	5	5	6	5	8	3	86
Threat		0	0	0	0	0	0	1	1	0	1	2	1	6
Trespassing		0	1	0	0	0	0	1	0	0	0	0	0	2
Vandalism		1	0	1	1	0	2	1	0	0	0	0	1	7
<b>Total</b>		<b>238</b>	<b>203</b>	<b>193</b>	<b>289</b>	<b>262</b>	<b>273</b>	<b>289</b>	<b>283</b>	<b>280</b>	<b>252</b>	<b>249</b>	<b>244</b>	<b>3055</b>

# Monthly Occurrence Report

For Period: 12/1/2009 to: 12/31/2009

Facility: **Sample Facility**

## Change Statistics by Category

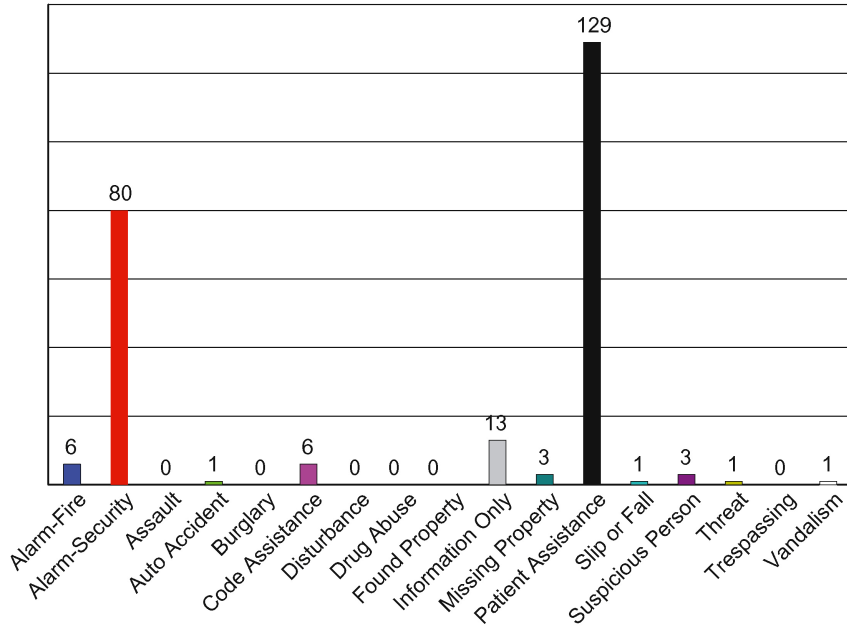
Category	Last Mo.	This Mo.	% Change	Last YTD	This YTD	% Change
Alarm-Fire	10	6	-40.0	119	74	-37.8
Alarm-Security	66	80	21.2	299	546	82.6
Assault	2	0	-100.0	6	15	150.0
Auto Accident	1	1	0.0	13	16	23.0
Burglary	1	0	-100.0	3	1	-66.6
Code Assistance	5	6	20.0	197	42	-78.6
Disturbance	0	0	0.0	44	14	-68.1
Drug Abuse	0	0	0.0	1	2	100.0
Found Property	0	0	0.0	1	2	100.0
Information Only	17	13	-23.5	228	225	-1.3
Missing Property	1	3	200.0	54	45	-16.6
Patient Assistance	136	129	-5.1	1,961	1,963	0.1
Slip or Fall	0	1	--	8	9	12.5
Suspicious Person	8	3	-62.5	71	86	21.1
Threat	2	1	-50.0	7	6	-14.2
Trespassing	0	0	0.0	1	2	100.0
Vandalism	0	1	--	17	7	-58.8
<b>Totals</b>	<b>249</b>	<b>244</b>	<b>-2.0</b>	<b>3030</b>	<b>3055</b>	<b>0.8</b>

# Monthly Occurrence Report

For Period: 12/1/2009 to: 12/31/2009

Facility: **Sample Facility**

# of Incidents by Category



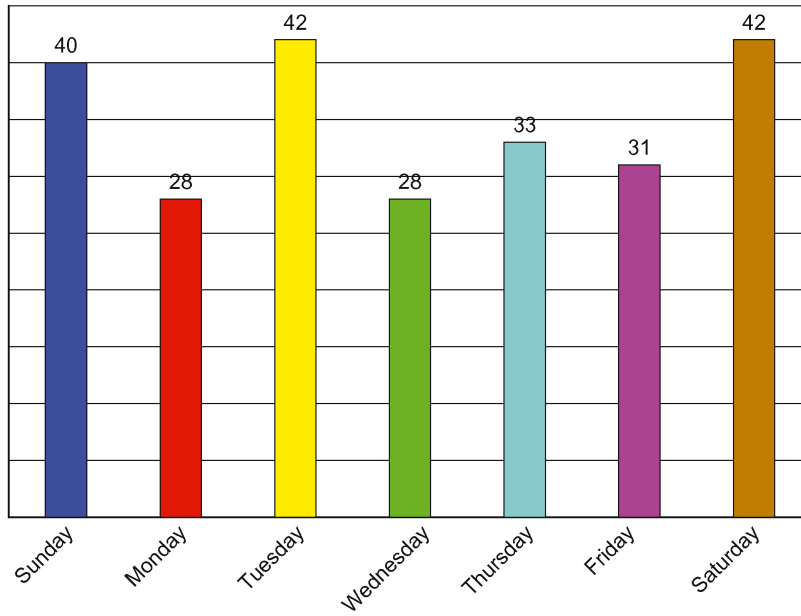
# Monthly Occurrence Report

For Period: 12/1/2009 to: 12/31/2009

Facility: **Sample Facility**

---

# of Incidents by Day of the Week



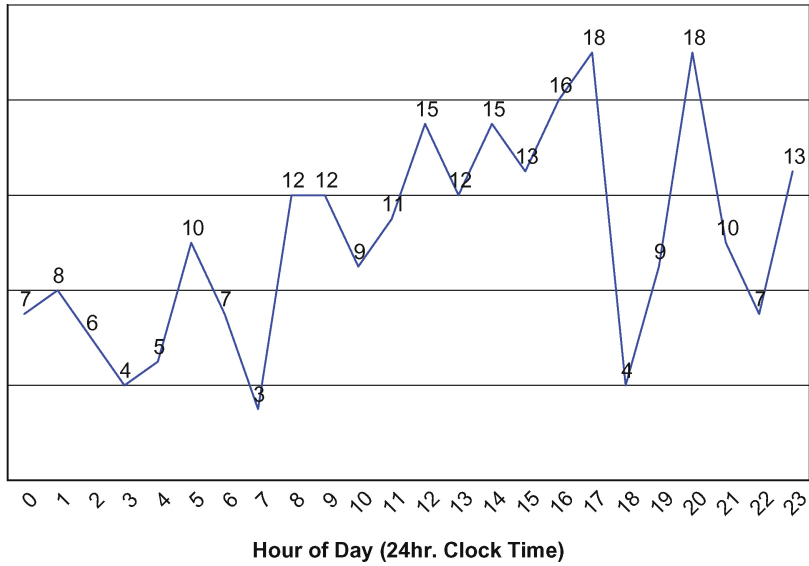
# Monthly Occurrence Report

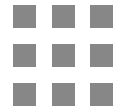
For Period: 12/1/2009 to: 12/31/2009

Facility: **Sample Facility**

---

# of Incidents by Hour of the Day





# Appendix II

## Sample

### Security Services Request for Proposal

#### Table of Contents

1. Introduction
  2. Instructions for Submitting Proposals
  3. Scope of Work
  4. Requirements
    - 4.1 Company Qualifications
    - 4.2 Management Team
    - 4.3 Staffing
    - 4.4 Crime Prevention
    - 4.5 Transition Plan
    - 4.6 Emergency Preparedness
    - 4.7 Technology
    - 4.8 Quality and Satisfaction Measurement
    - 4.9 References
    - 4.10 Financial Proposal
    - 4.11 Terms and Conditions
- Appendices:
- A. Scope of Work
  - B. Current Job Descriptions
  - C. Terms and Conditions

## 1. Introduction

United Memorial Hospital (UMH) will review proposals for Security Services in the following buildings:

- Main Hospital
- Women's and Children's Hospital
- Outpatient Psychiatry
- Methadone Clinic
- Madison Parking Garage
- Heart Institute
- Cancer Center
- MOB I, II, & III
- Physician & Administrative offices
- 11 community clinics

### Our Mission

UMH is an integrated, efficient, high-quality health care system where the patient comes first. We are an organization of caregivers who aspire to consistently high standards of quality, cost-effectiveness and patient satisfaction. We seek to improve the health of the communities we serve by delivering a broad range of services with sensitivity to the individual needs of our patients and their families.

### The Campus

UMH is located in downtown Seattle in a high profile area near key business, shopping, and tourist activity. It is a nationally recognized facility with 509 inpatient beds and a wide variety of clinical specialties, and is a Level I Trauma Center. The UMH campus covers several blocks, including bridge and tunnel connections between the UMH buildings. Additional information is available at [www.UMHcares.org](http://www.UMHcares.org).

## 2. Instructions for Submitting Proposals

### Schedule

- |                       |                                       |
|-----------------------|---------------------------------------|
| • Week of March 1–5   | Required site tours                   |
| • March 12            | Vendors return signed Confidentiality |
| • March 15            | Agreements                            |
| • April 1–2           | RFP distributed to Vendors            |
| • April 16, 1:00 P.M. | Optional site tours                   |
| • April 30, 1:00 P.M. | Final date for submission of written  |
| • Week of May 3       | questions                             |
| • May 17              | Proposals due                         |
| • May 31              | Presentations to Selection Committee  |
| • July 1              | Notify Vendor of intent to negotiate  |
|                       | Contract signed                       |
|                       | Commencement of Services              |

## Conditions

- All expenses incurred in the preparation of the proposal are the responsibility of the Vendor.
- The information contained in this Request for Proposal or acquired during the RFP process is confidential and shall not be communicated to any person or entity beyond what is required to prepare the proposal. All confidential information remains the property of UMH and must be destroyed or returned to UMH upon UMH request. All vendors are required to sign and return an UMH Confidentiality Agreement prior to receipt of this RFP.
- UMH reserves the right to award to any potential Vendor, or to none of the responding firms.
- All proposals shall be the property of UMH.
- Proposals shall be valid for 120 days after submission deadline.

Send questions regarding the RFP in writing via email to the address listed below by Friday April 30 at 1:00 PM: [MaterialsMgmtSecurity@UMHcares.org](mailto:MaterialsMgmtSecurity@UMHcares.org)

All Questions will be answered by \_\_\_\_\_, or other individuals identified as formal UMH contacts for this RFP process. Questions should not be directed to other UMH staff. Failure to comply with this requirement may result in disqualification.

Provide 2 signed copies of the proposal with an additional copy suitable for xero-graphic reproduction no later than 1:00 pm on Friday, April 30 to:

Director, Sourcing and Procurement  
 United Memorial Hospital  
 900 S. Broadway  
 Seattle, WA 98104  
 Attn: Rick James

Provide electronic copy of the complete proposal via email to [rjames@UMHcares.org](mailto:rjames@UMHcares.org), no later than 1:00 pm on Friday, April 30.

The Selection Committee includes representatives from the Emergency Department, Psychiatry, Women's Health, Physicians Group Practice, Human Resources, Support Services, and Administration. Each potential Vendor will have an opportunity to meet with committee members during the tour of the facility. A short list of Vendors will be invited to make a formal presentation to the selection committee during the first week of May.

UMH plans to award a three-year contract to the successful vendor, which will contain an option for two extensions of one year each.

## 3. Scope of Work

### Areas Included in Scope

Vendors are invited to provide a proposal for a Security Services program, including management and staff, in the UMH facilities listed in the Introduction, Section 1 of this



document. Current staffing requirements are attached to this document as Appendix A. Other services may be requested by UMH on an as-needed basis.

Each potential Vendor will be required to tour UMH and review the areas included in the Scope of the agreement during March. Each Vendor will have an opportunity for an optional second tour during early April.

Items that are performed by UMH Security Services that might be considered non-traditional Security functions include:

- Validate parking for all patients, visitors, clergy, and On-Call personnel 24/7.
- Issue Agency Nurse ID Badges after hours and document accurately.
- Issue Vendor badges and document accurately.
- Adhere to EMTALA by escorting patients to the ED.
- Provide Concierge services, giving hotel and restaurant information to visitors and patients.
- Provide mobile escorts to patients, staff, and visitors.
- Customer Service Officers working the 1st and 2nd floor Information Desks.

## Staffing

The Security Services management firm currently provides Management, Security Officers, and Customer Services Officers. The base scope of this RFP includes all those positions.

- Current staffing assumptions are included as Appendix A. Note that all FTE counts in that document are Productive Hours.
- Current Job Descriptions are included for your information as Appendix B.

Security Officers at UMH do not utilize guns or chemical weapons. Supervisory staff carry Tasers.

The following immunizations are required for contract employees prior to being assigned a position at UMH. The immunizations are administered by UMH Corporate Health, and the Vendor assumes the cost for those services. The list below is subject to change.

- Post offer screening
- MMR
- Respiratory fit questionnaire
- Follow up as needed for a potentially positive MMR or Tuberculosis
- TB skin injection
- Respiratory fit test
- Hepatitis B (employee option)

## Equipment

The Security Services vendor should provide a security patrol vehicle. UMH reimburses the vendor for the vehicle cost. It is primarily used for exterior patrols of UMH buildings.

It is also used to transfer patients as necessary between Outpatient treatment, Inpatient Psychiatry, and the Emergency Department. Examples of typical mileage are:

July, 2009

Daily mileage: 38–57 miles

November, 2009

Daily mileage: 25–31 miles

All other equipment is owned by UMH, including radios and communication equipment.

## Statistical Information

Fiscal Year 2009 volumes:

- Inpatient admissions—34,182
- Emergency Department visits—69,560
- Employees—3,144
- Deliveries—7,498
- Outpatient registrations—321,264
- Physicians—571

## 4. Requirements – Bidders Shall Respond to Each Point Below

### 4.1. Company Qualifications

4.1.1. *Briefly* describe company history, culture, values and business philosophy. Provide details of company size, resources, recent growth, innovations, business objectives and other information relevant to your firm's qualifications.

4.1.2. Discuss the firm's background in providing Security Services to healthcare organizations, particularly in academic medical centers, Level 1 Trauma Centers, behavioral health facilities, large birthing centers and urban locations.

4.1.3. Define what differentiates your firm from competitors. Discuss innovative programs in training, benefits, technology or other areas.

4.1.4. UMH reserves the right to restrict consideration of proposals to those firms which, based on their proposals and capabilities, have the depth and range of services to adequately provide the services.

### 4.2. Management Team

4.2.1. The successful firm will provide the Director and Managers for the Security Services program. Provide an organizational chart and job descriptions for the on-site management team to be assigned to UMH.

4.2.2. The Director will function and be recognized as a department head at UMH. That individual will formally report to the Director of Operations and Support. The Director and Managers will perform in accordance with UMH's written policies and procedures.

4.2.3. UMH will interview and approve potential Director and Manager candidates. Include resumes for potential Director and Manager candidates in the proposal.

4.2.4. Identify minimum qualifications required for each job description on the organizational chart.

4.2.5. Identify technical support available to the on-site management team. Describe initial and ongoing training programs for management.

4.2.6. Identify Vendor corporate/organizational leadership responsible for the UMH account. Include resume of that individual(s).

4.2.7. Describe the firm's ability to provide an Investigator and Expert Witness on matters related to Security at UMH.

4.2.8. Security Services representatives sit on the following UMH committees: Environment of Care, Safety, Emergency Department, Department of Psychiatry, Emergency Management, Emergency Response Team, Locksmith and Access Control Committee, Infant Abduction Safety committee, and Neighborhood Watch Committee (Local businesses and residential communities)

### 4.3. Staffing

#### 4.3.1. Recruitment:

- What are the minimum qualifications for Security Officers hired by your firm?
- What screening processes are performed prior to hiring?
- After an employee is hired, what processes are utilized to periodically verify current information?
- How will the selection process incorporate the specific culture and needs of UMH?
- How is diversity addressed and managed during recruitment and retention?

#### 4.3.2. Training:

- Describe new Security Officer training, including content overview, hours, teaching method, verification process
- Discuss customer service philosophy and training.
- Discuss your firm's philosophy in managing at-risk patient behavior. What training is provided to Officers, particularly in the Emergency Department and Behavioral Health areas? What guidelines and/or restrictions are provided to Officers?
- Discuss training to ensure that employees are able to work in a hospital setting.
- Discuss training related to OSHA, EPA, or other regulatory requirements.
- Discuss post assignment training and how individual officer competency is verified.
- What is the continuing education plan for personnel assigned to UMH, and what formal competency tests are provided?
- How is IAHS certification utilized in training or retention programs?

#### 4.3.3. Retention

- Describe your professional development program available to Security Officers and Security Leadership, and potential benefits to UMH.
- What is the officer turnover rate?
- What incentives are utilized to retain employees?
- What employee recognition programs are utilized?

#### 4.3.4. Benefits

Discuss the benefit program offered to staff assigned to UMH, including

- Health Care
- Vacation, Sick time
- Incentive programs
- Dental, Vision
- Tuition assistance
- Retirement

#### 4.3.5. Uniforms

- Provide description or images of the proposed uniform for Security Officers, Supervisors, and Customer Service Officers. Identify any proposed changes from the current UMH uniform.

#### 4.3.6. Union Membership

- Will Security Officers be union members? If so, specify the union.

#### 4.3.7. Organizational Chart

- Include an organizational chart and job description for each position recommended at UMH.

### 4.4. Risk Assessment/Crime Prevention

#### 4.4.1. Risk Assessment

- What are the top five security vulnerabilities for UMH, based upon its urban location, services it provides, and populations it serves?
- Were any observations made during the facility tour that supported this assessment of potential vulnerability?
- How does the firm manage security risk assessments? What information is collected?
- Who will manage the assessment?
- What Security Best Practices may be implemented at UMH?

4.4.2. Describe your philosophy and experience with lethal and less than lethal use of force tools in a health care setting.

4.4.3. Describe your philosophy and experience with metal detectors in a health care setting.

4.4.4. What programs does your firm offer to encourage participation of Non-Security staff in the overall Security program?

4.4.5. Discuss educational and security awareness programs that could be offered to UMH staff.

## 4.5. Transition Plan

4.5.1. Implementation of the Security Services management program at UMH must be achieved seamlessly, without disruption to ongoing patient care. Measurement of quality metrics will begin on the first day of the engagement.

4.5.2. Describe proposed transition plan, including discussion of staffing, workplan, training for Officers and UMH staff, schedule, ongoing quality measurements, and communications to Administration, Patient Care and other stakeholders.

4.5.3. Provide a timeline for implementation process, including required time between contract award (i.e. contract signatures) and implementation date.

4.5.4. What resources and information will be required from UMH to ensure a smooth transition?

## 4.6. Emergency Preparedness

4.6.1. Describe your experience in designing, conducting, and evaluation of emergency preparedness exercise related to security or other incidents.

4.6.2. Describe the firm's knowledge of The Joint Commission (TJC) accreditation standards.

- Provide examples of compliance documentation.
- Outline your experiences with participation in Environment of Care or Emergency Preparedness programs.
- Provide examples of demonstrated successes from recent TJC surveys. Describe lessons learned that will benefit UMH.
- Provide example of recommendations for improvement from TJC at hospitals for which your firm provides Security Services. How were those resolved? Describe lessons learned that will benefit UMH,
- Describe how your firm will approach the changes to the Security related EOC standards that became effective in 2009.

## 4.7. Technology

4.7.1. UMH will purchase technology for the Security Services program. Funding is obtained via the hospital's capital budget process. Proposed Security technology projects compete with other potential projects for funding allocation.

4.7.2. Describe technology upgrades that may be recommended at UMH, including but not limited to the areas listed below. What additional survey activity may be required

prior to finalizing these draft recommendations? What is the proposed schedule to prepare the final recommendations for updating of existing systems, where required?

- Command center
- Card readers
- Infant protection systems
- Incident reporting
- Recording and/or or archiving of appropriate systems above
- Cameras
- Alarm systems
- Key controls
- Communications equipment and systems

4.7.3. Describe your firm's expertise in design and installation of Security technology programs.

4.7.4. What third party technology vendors does your firm typically work with? Is there a financial relationship or an ownership position between those firms?

## 4.8. Quality and Satisfaction Measurement

4.8.1. Describe the key elements of your Quality Management processes, with an example of a written plan.

4.8.2. What capabilities will be provided for incident reporting and trending reports? What analyses will be provided to UMH management?

4.8.3. What metrics does your firm utilize to measure quality of services, both internally and externally?

4.8.4. How are customer satisfaction surveys and customer feedback incorporated in the Security Services program?

4.8.5. The UMH Vice President of Operations and the Director of Support Services will develop annual budgets and performance goals for the Security Services program each fiscal year. What metrics does your firm recommend be utilized to measure customer services and performance at UMH?

## 4.9. References

4.9.1. Provide five references of comparable organizations where the firm manages Environmental Services. Include at least one reference in the Seattle area. Include contact names, phone numbers, email addresses, approximate size of contract, and date that services began.

4.9.2. UMH may request site visits to one or more reference accounts.

## 4.10. Financial Proposal

4.10.1. The Financial Proposal shall cover all costs for the Security Services program.

4.10.2. For each job classification in the proposed organization chart (both management and staff)

- Propose target salary for each job classification.
- Identify target benefit cost for each job classification.

4.10.3. Identify proposed initial capital cost and ongoing operational costs for technology upgrades.

- Discuss which programs are most important to successful implementation of a Security program at UMH.
- Discuss which programs might have impact on FTE counts or assignments.
- Discuss how the success of each proposed technology investment will be documented or measured.

4.10.4. Identify vehicle cost, and any other costs not included above.

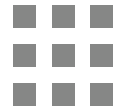
4.10.5. Provide summary of all program costs, with total for first year, second year, and third year.

4.10.6. Define what portions of the financial proposal that will be at risk based upon non-satisfactory performance of Quality and Performance metrics or budget goals.

4.10.7. UMH continues to be an expanding organization, with several major expansion projects planned for the next few years. Describe the metrics and method to be used in planning for opening of additional areas in the future if additional Security staff and managers are required to support the new functions, both to document staffing levels and fee.

## 4.11. Terms and Conditions

4.11.1. The Draft contract Terms and Conditions is included in this RFP (Appendix C). Provide statement of agreement to those terms, or provide red-line markup in Word form with the proposal.



# Index

## A

- Abductions, *see also* Infant abductions  
abductor methods, 511–512  
abductor profile, 511–512  
definition, 63  
patients, 43  
security risks, 51, 53f, 63, 80f  
security sensitive areas, 505–506  
video surveillance, 462  
visitor violence, 489  
workplace violence, 643
- Aberrant behavior, unreported, 403–404
- Access control  
after-hours visitors, 356  
bomb threat prevention, 602  
CCTV setup, 461f  
chain link fencing, 426  
as challenge, 454–458  
child development centers, 556–557  
computer-based key accountability, 433–434  
CPTED, 441  
ED security, 533, 534f  
electronic security systems, 455  
electronic systems, 430–431  
emergency planning, 616  
employee lockers, 122  
external protection planning, 611–612  
IAHSS guidelines, 381–382  
importance, 637–638  
infant security, 519, 644  
intercoms/video door phones, 457–458  
large acreage facilities, 357  
laundry, 554  
lockdown, 456–457  
locked areas, 121–122  
managed, 458  
off-campus facilities, 570–571  
overview, 120–122  
parking areas, 587  
pharmacies, 541  
security sensitive areas, 456, 507  
stages, 617t  
storerooms, 550  
surface parking lots, 579–580  
technologies, 455t  
video surveillance recording, 468
- Accidents  
disasters, 72  
emergency events, 614–615  
fires, 72  
investigation methods, 117–118  
prevention, 26  
reporting system, 26, 117–118  
as safety risk, 66–67
- Accountability issues  
access control, 120, 454  
badges, 514  
cash/payment handling, 575  
employee entry, 445  
equipment, 551  
key control, 433–434, 435  
minor crimes, 409  
missing patients, 322  
package inspection, 386  
patient property, 69–70, 352  
patient whereabouts, 65  
performance expectations, 191  
post assignments, 271  
property marking, 438  
property records, 301  
theft, 67
- Accreditation  
CMS program, 15  
security administration, 7  
security rationale, 21  
TJC approach, 9  
TJC scoring, 10  
TJC sentinel events, 11
- Accreditation Canada, 44
- Accreditation Watch, 12–13
- ACEP, *see* American College of Emergency Physicians (ACEP)
- Acetone, prescription altering, 544
- Acrylic plastic glass protection, 437
- Active shooter events  
basic issues, 613–614  
Doctor's Hospital case, 454–455  
emergency preparedness, 592t  
security communications, 614  
staff actions, 614  
Virginia Tech tragedy, 14–15, 474, 641
- Acute care units  
assaults, 462  
behavioral health patients, 341  
definition, 3  
officer vulnerability, 207  
security safety/assessment, 499  
video surveillance, 462
- ADA, *see* Americans with Disabilities Act (ADA)
- Admissions  
ED security, 531–532  
patient property security, 351–352  
video surveillance, 462
- Advanced Training Manual for Healthcare Security Personnel*, 249
- Adversarial interviewing, definition, 417–418
- Adverse selection theory, background checks, 380
- Advertising, officer recruitment, 181f, 182
- After-Care Professional Nurses Registry of California, 566
- After-hours access control  
considerations, 456  
importance, 638  
pharmacies, 542  
storerooms, 550
- Afternoon-shift employees, parking options, 586
- Age factor, as psychological deterrents, 28
- Aggravated assault  
definition, 52  
workplace violence, 491f
- Aggression management  
ED security, 539  
new officer training, 243t  
security role, 241–243, 631
- Aggressive behavior  
de-escalation, 184, 241–243  
escalation, 644  
legislative action, 499  
management training, 243t, 261, 497  
prevention/management, 88–89  
security staff criteria, 630t  
security watch, 330
- AIDS patient security, 336–338
- Air packs, patrol vehicle equipment, 284
- Alarm monitoring  
central security station, 447  
as community outreach, 103  
infant security, 521, 521t  
redundant, 519  
shared central station, 449–450
- Alarm systems  
basic applications, 452–453  
central security station, 448  
components, 451–452  
duress codes, 453  
in electronic security, 450–454  
false alarms, 453–454  
gift shops, 559  
inspection, 123–124  
life-safety focused doors, 445  
off-campus facilities, 571  
pharmacies, 540–541  
positioning, 638  
proprietary, 453
- Alertness, as crime deterrent, 404
- Alexian Brothers Hospital (IL), 320
- ALF, *see* Animal Liberation Front (ALF)
- Altered prescriptions, pharmacies, 544
- Alzheimer's patients, security role, 348
- AMA, *see* American Medical Association (AMA)
- Ambassador uniform style, characteristics, 202–203
- Ambulance entrance  
ED security, 533, 534f  
parking areas, 531  
visitor contact, 353
- Ambulance services, and linen loss, 553
- American College of Emergency Physicians (ACEP), 339, 500
- American College of Physicians, 8
- American College of Surgeons, 8
- American Dental Association, 8
- American Hospital Association (AHA), 8, 479
- American Medical Association (AMA), 8, 324
- American National Standards Institute (ANSI), 41
- American Osteopathic Association (AOA), 15
- American Society for Healthcare Engineering (ASHE), 160
- American Society for Healthcare Risk Management (ASHRM), 609
- Americans with Disabilities Act (ADA), 186
- Ammunition, arming officers, 212–213
- Analog cameras  
*vs.* digital, 464, 465f  
video surveillance, 463
- Andragogy model, 232
- Anesthesia-type drug abuse, 58–59
- Animal Liberation Front (ALF), 554–555, 555–556



- Animal research laboratories
    - employee background checks, 555
    - infiltration methods, 555–556
    - protection, 554–556
    - security sensitive areas, 505, 506
  - Animal rights activists
    - infiltration methods, 555–556
    - protection from, 554–555
  - Annunciators, alarm systems, 451
  - Anschutz Medical Campus (CO), 122–123
  - ANSI, *see* American National Standards Institute (ANSI)
  - Antibody profiling, infant identification, 513
  - Anti-Drug Abuse Act, 391
  - Anti-passback parking control, 587
  - Antivivisectionists, 554–555
  - AOA, *see* American Osteopathic Association (AOA)
  - Apathy, as security issue, 403–404
  - APPL, *see* Area Police/Private Security Liason (APPL)
  - Applicant issues, *see also* Background checks
    - application form design, 377–378
    - deceptive information, 379
    - suitability information, 377–378
  - Applying ICS to Healthcare Organizations (IS-200), 254–255
  - Area Police/Private Security Liason (APPL), 361
  - Armed robbery
    - deployment plan, 267
    - parking control, 577
    - pharmacies, 540
    - security policies, 647t
    - as security risk, 65
    - security sensitive areas, 505
    - security training, 397
  - Arson attack, glazed glass protection, 436
  - The Art of Successful Security Management* (Dalton), 132
  - Artwork, alarm protection, 450–451
  - ASHE seminars, 162
  - ASHRM, *see* American Society for Healthcare Risk Management (ASHRM)
  - ASIS International
    - required reading, 160
    - security program factors, 41
    - seminars, 162
    - staff security education, 397
  - ASPR, *see* Assistant Secretary for Preparedness and Response (ASPR)
  - Assaultive behavior
    - identification, 497
    - managing, 486
    - security staffing criteria, 630t
  - Assaults
    - communication devices, 216
    - critical incident response plan, 507–508
    - definition, 52
    - ED security, 528
    - employee expectations, 270
    - employee security knowledge, 402
    - ICUs, 559
    - incident increase, 19, 622, 624
    - incident reporting, 305f, 402
    - investigation, 407–408
    - legislative action, 499
    - natural surveillance, 441–442
    - neighborhood stability, 102–103
    - officer authority, 177
    - officer liability, 322–323
    - parking control, 578, 579, 587
    - as patient protection event, 43
    - patients, 487–488
    - physicians, 563
    - premeditated, 644
    - prosecution, 500
    - risks/vulnerabilities, 627
    - security performance, 96t
    - as security risk, 51, 52, 52–54
    - security risk worksheet, 80f
    - security signage, 441
    - security staffing, 630t
    - staff flexing plan, 266
    - during strikes, 64
    - threat assessment, 81f
    - as TJC sentinel event, 12, 13f
    - types, 486
    - from verbal arguments, 57
    - video surveillance, 462
    - by visitors, 489
    - vulnerability, 207, 273
    - workplace violence, 484, 485, 485–486, 497, 642, 484t, 491f
    - work-related, 486
  - Assertiveness, officer traits, 184f
  - Asset tracking
    - equipment, 551
    - purpose, 641
    - via RFID, 475–479
  - Assistant Secretary for Preparedness and Response (ASPR), 597
  - Assisted living
    - definition, 2
    - electronic access control, 458
    - intercom systems, 458
    - security service impact, 129f
    - TJC standards, 8t
  - Assurance, RATER model, 245
  - At-risk patients
    - Blue Shirt Program, 349–350
    - deployment objectives, 267–268
    - ED security design, 531
    - ED security education, 538t
    - ED staffing, 537
    - ICU, 340
    - interaction protocols, 536–537
    - management, 241–243, 244, 536–537
    - metal screening, 479
    - officer arming trends, 213
    - quiet/observation room, 533–534
    - restraint training, 244
    - risk assessment, 80f
    - security involvement, 633–634
    - security staffing, 630t
    - security watch, 329–330, 331
    - specialized sitters, 203
    - workplace violence, 483
  - Attendance monitoring, 169
  - Attire, *see* Uniforms
  - Attitude
    - employees toward safety, 404–405
    - officer selection criteria, 183
    - performance monitoring, 171–172
  - Audits
    - as nonincident-driven investigation, 415
    - overview, 123–124
    - pharmacy drugs, 542
    - and risk assessment, 73
    - testing, 123–124
  - Australia
    - behavioral health patients, 341–342
    - OC spray, 221
    - security program factors, 45
    - violence perpetrator prosecution, 500
    - workplace violence, 485
  - Australian Commission on Safety and Quality in Healthcare Care, 45
  - Authorities Having Jurisdiction (AHJ), 42
  - Autistic patients, 342–344, 343t
  - Automated dispensing machines, 543–544
  - Automated parking control, 587
  - Auto thefts
    - home caregivers, 566
    - prevention, 398t
    - as security risks, 56
- B**
- Baby switching problem, 71
  - Baby viewing areas, abductions from, 511
  - Background checks
    - animal research labs, 555
    - applicants, 119, 378–379
    - child development centers, 556–557
    - employees, 119
    - as nonincident investigation, 414–415
    - officer selection process, 186
    - screeners, 379–380
    - security strategic plan questions, 102
    - service providers, 379–380
    - staff selection, 377
  - Badges, *see* Identification badges
  - Baldwin Area Medical Center (WI), 55
  - Banner Health's Thunderbid and Estrella Hospital (AZ), 284–286
  - Banner notifications, 478f
  - Baptist Hospital (MS), 489
  - Barbed-wire fencing, 426
  - Barcode scanners, visitor management systems, 471
  - Barnes-Jewish Hospital (MO), 251–252
  - Barriers
    - bollards, 428
    - chain link fencing, 426
    - child development centers, 556–557
    - decorative metal fencing, 426–427
    - ED security, 531
    - fencing, 424–427
    - as physical safeguards, 424–428
    - tree/shrub, 429–430
  - Basic Elements of Healthcare Security Management*, 258
  - Basic Training Manual for Healthcare Security Officers*, 247
  - Bates, Norman, 298–299
  - Batons
    - equipment carried, 224
    - use of force options, 636
  - Battery-jumping service, 282–284
  - Battle dress uniform (BDU), 203
  - Baylor Health Care System (TX), 143
  - Baystate Health (MA), 498
  - BDU, *see* Battle dress uniform (BDU)
  - Bed space
    - emergency employee housing, 618–619
    - hospitality types, 4
  - Behavior, *see also specific types*
    - acceptable, 28
    - autistic patients, 343–344
    - as contemporary event, 28
    - disciplinary action, 195–196
    - documentation, 175
    - and fear of punishment, 29
    - gangs, 252–253, 647t
    - and interaction techniques, 499
    - managing, 174
    - and officer selection, 185
    - on-the-job, 174
    - patient risk, 566
    - performance documentation, 173, 174t
    - performance expectations, 191
    - positive reinforcement, 192–193
    - psychological deterrents, 27
    - and security design, 637
    - security strategies, 569t
    - security watch, 329–330
    - societal acceptance, 28
    - staff selection, 376
    - via training, 233
    - uniform style effect, 201, 201t, 634
    - video analytics, 466
    - video surveillance, 469
    - workplace violence, 488–489, 497
  - Behavioral health facilities
    - arming security, 213

- bullet resistive glass, 437
  - duress alarms, 452, 638
  - fire prevention and control, 597
  - forensic patients, 345
  - funding reduction, 267–268
  - mass notifications, 474
  - officer disarming, 212
  - patient assistance, 322
  - patient risk groups, 334
  - patrol issues, 276–277
  - risk assessment data, 76f
  - risk posture self-assessment, 80f
  - security role, 341–342, 633–634
  - security watch, 331
  - uniform style, 202
  - video surveillance, 462, 470
  - violence, 483–484
  - visitor control, 354
  - workplace violence, 483–484, 492
  - Behavioral health patients
    - emergency department, 340
    - fire control, 597
    - security role, 341–342
    - threat response, 495
    - video surveillance, 462
  - Belly chains, forensic patients, 346
  - Ben Taub Hospital (TX), 56
  - Berry, Leonard, 245
  - Best practice, definition and examples, 47
  - Beth Israel Deaconess Medical Center (NY), 333, 610–611
  - Bicycle patrol, 280–281
  - Bicycle storage, 426
  - Biological weapons, 609–610
  - Biometrics
    - automated dispensing machines, 543–544
    - computer-based key accountability, 433–434
  - Birthing unit
    - discharge issues, 525–527
    - infant security, 527
    - security sensitive areas, 505, 506
  - Blankets
    - forensic patients, 345–346
    - patrol vehicle equipment, 284
  - Blazer uniform style
    - characteristics, 202–203
    - example, 203f
    - as option, 634
  - Block parties, as community outreach, 103
  - Blood-borne pathogens, 246
  - Blue Shirt Program, 349–350
  - Boatwright, Waneta, 65
  - Body of knowledge
    - accessing, 46–48
    - alarm systems, 450
    - best practice, 47
    - common goals, 48
    - definition, 45–48
    - development, 45–46
    - ISP, 46–47
    - security administrators, 162
    - standard of care, 48
  - Body language
    - with autistic patients, 344
    - officer response, 292
    - types, 498–499
    - use of force, 635t
  - Bollards, physical security, 428
  - Bomb threat plan
    - bomb search, 603–604
    - documentation, 605
    - emergency preparedness, 601–605, 592t
    - emergency termination, 604–605
    - establishing authority, 602
    - evacuation, 604
    - prevention, 602
    - security risks, 54–55
    - steps, 602
    - threat reception, 602–603
  - Boulder Community Hospital (CO), 542–543
  - Bribery, for infiltrations, 555
  - Brick wall barriers, 424, 427f
  - Brochures, officer recruitment, 180–181
  - Brockton Hospital (MA), 486
  - Brookwood Medical Center (AL), 489
  - Broom, patrol vehicle equipment, 284
  - BSIS, *see* California Bureau of Security and Investigative Services (BSIS)
  - Buchman, Tracy, 470
  - Building construction
    - security design, 446
    - security staffing, 154
    - security strategic plan, 106
  - Bulletins, training, 260f
  - Bullet-resistant glass
    - pharmacies, 541
    - as safeguard, 437
  - Bullhorn notifications, 478f
  - Bureau of Building Inspection, 578
  - Burglary
    - patient property, 351–352
    - pharmacies, 540
    - ram-raiding, 428
    - security performance measurement, 96t
    - as security risk, 53f, 55–56
    - threat assessment, 81f
  - Business improvement districts (BIDs), 371
  - Business knowledge, management selection, 163
  - Business offices
    - security concerns, 557
    - violence risks, 492
  - Butler, Alan, 494
- ## C
- Cabinets
    - computer-based key accountability, 433–434
    - pharmacies, 542
  - California Bureau of Security and Investigative Services (BSIS), officer licensing, 178–179
  - Call boxes, *see* Emergency call boxes
  - Canada
    - security program factors, 44–45
    - violence perpetrator prosecution, 500
    - workplace violence, 485
  - Canadian Medical Association, 221
  - Canine patrol, 284–286
  - CAP Index
    - CRIMECAST® reports, 208
    - employee education, 399
    - security risk assessment, 76
  - “Care for Patients – Protect their Personal Data” campaign, 558–559
  - Carolinas HealthCare System (CHS), 281, 595, 596f
  - The Carrell Clinic (TX), 558
  - Case report, *see* Security incident report (SIR)
  - Cash handling
    - off-campus security, 575–576
    - officer arming factors, 207
    - protocol, 126–127
    - robbery risks, 65
    - storage in safes, 438
  - Cashiers
    - alarms, 638
    - parking structures, 582
    - security concerns, 557
  - Catastrophic reaction, wandering patients, 348
  - Cavalier, Debra Higgins, 555
  - CCD, *see* Charge-coupled device (CCD)
  - CCTV, *see* Closed circuit television (CCTV)
  - CCW, *see* Concealed carry weapons (CCW)
  - CDC, *see* The Centers for Disease Control (CDC) Prevention
  - Celebrity patients, 334
  - Cell phones
    - duty belt, 225
    - emergency messages, 126
    - off-campus security, 567
    - for security communications, 116, 216
  - The Centers for Disease Control (CDC) Prevention, 342
  - Centers for Medicare and Medicaid Services (CMS)
    - anti-staff violence, 7
    - chemical agent guidelines, 224
    - forensic patients, 254, 344–345
    - incident reporting, 402
    - overview, 15–16
    - patient care unit surveillance, 470
    - restraint training, 244
    - security programs, 38, 42, 624
    - Taser regulations, 220–221
    - use of force options, 636
    - workplace violence, 488–489, 642–643
  - Central Florida Regional Hospital, 523–524, 622
  - Centralization
    - security strategic plan questions, 101–102
    - systems security programs, 135, 146
  - Central Philadelphia Development Corporation, 371
  - Central security station
    - advantages, 447–448
    - alarm systems, 451
    - cost, 449–450
    - design, 448
    - emergency call boxes, 474
    - example, 448f
    - shared, 449–450
  - CEO, *see* Chief executive officer (CEO)
  - Certified Healthcare Protection Administrator (CHPA)
    - credentialing programs, 161
    - security administrators, 161, 625
    - security risk assessment, 73
  - Certified Healthcare Security Supervisor (CHSS), 250
  - Certified Nurse Assistant (CNA), 62
  - Certified Protection Professional (CPP)
    - credentialing programs, 161
    - exam, 162
    - security administrator traits, 625
    - security risk assessment, 73
  - Chain, patrol vehicle equipment, 284
  - Chain link fencing, 426
  - Charge-coupled device (CCD), 463
  - Charleston Area Medical Center's Memorial Hospital (WV), 489, 621
  - Check-off form reports, 300
  - Chemical agents
    - equipment carried, 221–224
    - as use of force, 635t
  - Chief executive officer (CEO), 131
  - Chief operating officer (COO), 131
  - Child abduction
    - drills and exercises, 525
    - new employee training, 396
    - protection strategies, 528t
    - risk areas, 510–511, 644
    - security plan, 512
  - Child abuse
    - child development centers, 556–557
    - family abductions, 527
    - MBPS, 350–351
    - security involvement, 350–351

- Child development centers
  - abductions from, 510–511
  - security concerns, 556–557
- Child pornography, 52–54
- Children's Hospital (CO), 472
- Children's Hospital (WI), 469
- Chiller towers, 426
- CHPA, *see* Certified Healthcare Protection Administrator (CHPA)
- CHS, *see* Carolinas HealthCare System (CHS)
- Cisley v. Longs Peak Association, et al.*, 471
- Civil actions, against officers, 177
- Civil disturbances
  - access control, 638
  - critical task list, 242f
  - dissident group actions, 56
  - emergency planning, 611–613, 592t
  - emergency preparedness, 592t
  - employee travel/housing, 618–619
  - external protection planning, 611–612
  - vs.* gang/mob activities, 610
  - handcuff use, 217
  - IAHSS officer training, 248t
  - internal protection planning, 612–613
  - lockdown, 456
  - off-duty law enforcement, 143
  - safeguards, 610
  - security risks, 53f, 56, 627
- Cleveland Clinic Foundation (OH), 58–59, 143
- Clock cameras, 467
- Closed circuit television (CCTV), *see also* Video surveillance
  - analog systems, 463–464
  - decentralized setup, 462f
  - dummy cameras, 470–471
  - example setup, 461f
  - IAHSS guidelines, 459
  - infant protection systems, 473
  - inspection, 123–124
  - IP cameras, 464
  - location and image quality, 638
  - monitoring, 468–469
  - patient care areas, 469
  - patient elopement, 327
  - via PDA, 228
  - as preventative patrol, 112
  - security staffing, 153
  - security strategic plan guidelines, 105
  - SMP 91f
  - video surveillance, 458
- CMS, *see* Centers for Medicare and Medicaid Services (CMS)
- CNA, *see* Certified Nurse Assistant (CNA)
- CN gas, 221
- Code of Federal Regulations, 539
- "Code Pink"
  - definition, 522
  - healthcare executive primer, 621
  - staff response, 523
  - vulnerable areas, 527
- Code systems
  - automated dispensing machines, 543–544
  - bomb threats, 603–604
  - emergency announcements, 615–616
  - infant abductions, 527
  - terrorism preparedness, 608–609
  - two-way radios, 216
- Colleges recruitment, 182
- Colorado Hospital Association, 367, 615
- Color coding
  - emergency announcements, 615
  - ID badges, 384
  - reports, 300
  - terrorism preparedness, 608–609
- Color posters, employee education, 398
- Combative patients
  - chemical agents, 221
  - disturbances, 57–58
  - in emergency department, 339–340
  - general nursing unit, 341
  - in ICUs, 340, 340–341
  - management, 647t
  - medical/dental clinics, 341
  - quiet/observation room, 533–534
  - as risk group, 334, 338–341
  - security performance, 187t
- Combination form reports, 300
- Command posts, for emergencies, 612
- Command signs, as physical security, 440
- Commissioned police officers, as security staff, 143
- Common sense, as crime deterrent, 404
- Communication devices
  - CHS trailer, 596
  - emergency messages, 126
  - equipment carried, 215, 216–217
  - internal protection planning, 612
  - law enforcement liaisons, 371
  - parking area security, 584
  - parking control, 579–580, 588, 578, 581–582
  - patrol vehicle equipment, 283
  - personal, 584
  - as safeguard, 28t, 81
  - safe room, 534–535
  - security layering, 424
  - security program effectiveness, 98
  - system of perimeters, 424
  - technology applications, 639
- Communications, *see* Security communications
- Communication skills
  - officer selection criteria, 179, 183, 185
  - security principles, 194f
  - supervisory training, 251t
- Community issues
  - arming officers, 211–212
  - facility security impact, 628–629
  - law enforcement liaison, 371
  - outreach programs, 102–103
  - relations with, 130
- Community provider services, 564–568
- Community Safety Cameras (CA), 462–463
- Compartmentalization, ED design, 531, 533
- Competency issues
  - leadership development, 257–258
  - new officer training, 239–240
  - security staff, 631–632
- Competency verification
  - new officers, 240–241
  - sample format, 240f
- Comprehensive Accreditation Manual for Hospitals*, 8
- Compressed medical gasses
  - nitrous oxide storage, 560
  - oxygen storage, 560
  - security concerns, 559–560
- Computer-based training
  - staff security education, 397
  - as training resource, 259
- Computer-generated reports, 300–301
- Computer hardware security, 64
- Concealed carry weapons (CCW), 202–203
- Concrete wall barriers, 424
- Conditions of employment, 30
- Confidence, officer traits, 184f
- Confidentiality
  - sample agreement, 195f
  - security principles, 194f
- Conflict resolution
  - training, 644
  - violence prevention, 498
- Conscious motivation, psychological deterrents, 29
- Conservation of resources, as security function, 125
- Consultants
  - IAHSS guidelines, 40
  - outsourcing basics, 141
  - security force deployment, 265
  - for security risk assessments, 73–74
- Contactless smart cards, 455t
- "Continuance," records importance, 296
- Contraband
  - hiding in landscaping, 427, 429–430
  - patient search guidelines, 333
  - policies, 390–391
  - transport suspicions, 387
- Contract security staff, *see also* Outsourced services
  - advantages/disadvantages, 139–142
  - background checks, 380
  - vs.* corporate approach, 145
  - emergency staffing, 617
  - licensing, 178–179
  - officer coverage, 571
  - overview, 139–142
  - patient assistance, 321
  - with proprietary staff, 142
  - records, 262
  - security division as, 143
  - security history, 23
  - staffing models, 138t
  - staff types, 136
  - training formats, 248–249
  - training funding, 233
  - training time, 152
- Control holds, as use of force, 635t
- Controlled Substances Act, 543
- Convergence
  - HIPAA overview, 14
  - IT security, 557–558
  - U.S. hospital security history, 24
- COO, *see* Chief operating officer (COO)
- Cook, Richard, 259
- Cord blood, infant identification, 513
- Corporate policy
  - security programs, 34–35
  - security staffing, 144–147
- Correctional personnel, forensic patients, 645
- Council on Safety, Security, and Emergency Preparedness, 160
- Counterproductive behavior, employee theft risks, 68
- Covert cameras, 467–468
- Covert investigations, *see* Undercover investigations
- CPP, *see* Certified Protection Professional (CPP)
- CPTED, *see* Crime Prevention through Environmental Design (CPTED)
- Credentialing programs
  - falsifying, 379
  - security administrators, 161
- Crevier, Mark E., 280–281
- CRIMECAST®, 208, 209f
- Crime Prevention Coalition, purpose, 393
- Crime prevention efforts
  - definition, 393
  - education programs, 397, 397t
  - handbills, 401f
  - handouts, 399, 399f, 400f
  - hospital watch, 405–406
  - meetings, 401
  - newsletters, 397–398, 398t
  - security fair, 401
  - security strategic plan, 102–103
  - websites/e-mail broadcasts, 398–401
- Crime Prevention through Environmental Design (CPTED)
  - basic concept, 441–442
  - ED security design, 531
  - fundamentals, 27–28
  - natural access control, 441

- natural surveillance, 441–442  
 security design, 637  
 territorial reinforcement, 442
- Crime triangle  
 diagram, 404f  
 employee knowledge, 403–404
- Criminal justice system, and security  
 strategic plan, 104
- Criminal record, applicants, 379
- Criminal violence, definition, 484
- Criminology, definition, 75
- Critical access hospital, characteristics, 4
- Critical incident response plan  
 infant abductions  
 basic plan, 522–525  
 communications/media relations,  
 524–525  
 drills and exercises, 525  
 facility-wide staff, 523  
 security staff, 523–524  
 unit nursing personnel, 522  
 security sensitive areas, 507–508
- Critical task focused training, 242f, 235–241
- C5 gas equipment, 221
- Cullen, Charles, 61
- Cultural issues  
 officer diversity, 185  
 staff scheduling factors, 269
- Curfews, emergency planning, 618–619
- Customer service  
 new officer training, 245  
 security expectations, 626  
 security greetings, 403  
 security programs, 111  
 security role, 632
- D**
- Daily activity report, 310f, 309–311
- Dallas/North Texas Regional Law  
 Enforcement and Security Program  
 (LEAPS), 361
- Dalton, Dennis, 132
- Damaged property, policy for, 390
- Daniel, Marc, 491
- Data analysis, security staffing, 152–154
- Data security  
 administrator responsibilities, 7  
 effectiveness, 443  
 information loss risks, 64  
 IT, 557–558  
 requirements, 443  
 TJC sentinel event, 12
- DEA, *see* Drug Enforcement Agency (DEA)
- Deadly force, as use of force, 635t
- Debbaudt, Dennis, 343–344
- Deceased patients, handling, 125–126
- Decentralization  
 CCTV surveillance, 460–461, 462f  
 security strategic plan questions, 101–102  
 systems security management control,  
 135–136
- Decision making abilities  
 security principles, 194f  
 security safeguards, 30
- Decorative metal fencing, 427f, 426–427
- Defensible Space* (Newman), 441
- Defensive medicine, definition, 2
- Delirium, wandering patients, 348
- Delivery people relationships, 130
- Dementia patients, security involvement,  
 348–350
- Demonstrations, security risks, 56
- Dental offices  
 as burglary target, 56  
 combative patients, 341
- Denver boot, 588, 589f
- Denver Police Department, 367
- Department of Defense, 608–609
- Department of Health and Human Services  
 (DHHS), 108, 558
- Department of Health and Human Services  
 (HHS), 14
- Department of Health and Social Security, 22
- Department of Labor, 289
- Department of Motor Vehicles (DMV), 119
- Departments of Public Safety, 143, 177
- Deployment plan, *see also* Patrols  
 administrative records role, 298  
 double coverage, 274  
 employee security knowledge, 403  
 factors, 270–271  
 medium-sized center, 275t  
 methods, 265  
 objectives, 267–268  
 operational *vs.* nonoperational periods,  
 275–276  
 post assignments, 271–272  
 sample schedule, 273  
 security staffing, 156, 147–149  
 small center, 275t  
 systems security programs, 146
- Deterrent value, firearms, 208
- Det Norske Veritas Healthcare, Inc. (DNV), 15
- DHHS, *see* Department of Health and Human  
 Services (DHHS)
- Diagnostic and Statistical Manual of Mental  
 Disorders (DSM), 186
- Digital displays, mass notifications, 478f
- Digital video recorders (DVRs)  
 micro DVRs, 467  
 video surveillance, 458, 463
- Director of Health Information Management,  
 548
- Director of Materials Management, 549
- Dirty bombs, 609
- Disaster risks, 72
- Discharge issues  
 infant security, 525–527  
 patients, 71
- Disciplinary action, officers, 195–196
- Disguises, activist infiltrations, 555
- Dismissal, as disciplinary action, 196
- Disorderly conduct  
 handling options, 111–112  
 as security risk, 57
- Dispensing machines  
 drug diversion/theft, 543–544  
 fuel, 426
- Disposal policy, equipment, 551–552
- Disruptive behavior  
 early symptoms, 536  
 ED security, 527–528  
 ED staff education, 538  
 gang members, 610  
 management training, 243  
 medical/dental clinics, 341  
 officer training for, 243, 536  
 orderly environment, 111–112  
 pandemic events, 613  
 patient care units, 276–277  
 security watch, 330  
 workplace violence, 483
- Dissident group actions, 56–57
- Disturbances  
 behavioral health patients, 342  
 civil, *see* Civil disturbances  
 combative patient, 57–58  
 emergency room, 365  
 ICU, 340–341, 559  
 incident reports, 305f  
 infant security, 515t  
 investigations, 409–410  
 medical/dental clinics, 341  
 off-duty employees, 385  
 security awareness, 92  
 security risks, 53f, 57–58
- DMV, *see* Department of Motor Vehicles  
 (DMV)
- DNV, *see* Det Norske Veritas Healthcare, Inc.  
 (DNV)
- Doctor's Hospital (GA), 454–455, 622
- Documentation, *see also* Records  
 bomb threats, 605  
 negative behaviors, 175  
 performance management, 173–176  
 policy, 298–299  
 reasons for, 174t  
 supervisor considerations, 175–176
- Dolan, Harry, 122
- Domestic violence patient  
 definition, 484  
 ED security, 527–528  
 officer training, 252t  
 threat response team, 495–496  
 VIP patients, 80f  
 and workplace violence, 483
- Double-coverage deployment plans, 274
- Double-lock systems, 291
- Drills and exercises  
 emergency preparedness, 594–596  
 infant abduction, 98, 526f, 525
- Driver's license readers, 471
- Driveways, ED security, 531
- Drug abuse  
 applicants, 379  
 ED security, 527–528  
 education programs, 391  
 employee paraphernalia, 31  
 fentanyl patches, 543  
 forged prescriptions, 544  
 investigation, 409–410  
 security audit, 415  
 security investigations, 409–410  
 security/police relationship, 360  
 as security risk, 53f, 58–59  
 workplace violence, 486
- Drug diversion  
 home patient security, 566  
 pharmacies, 542–544
- Drug Enforcement Agency (DEA)  
 applicant background investigation, 119  
 drug diversion/theft, 543  
 liaison with, 122
- Drug-Free Workplace Act, 391
- Drug testing policies, 391
- Drug theft  
 civil disturbances, 611  
 and drug abuse, 58  
 executive primer, 627  
 officer arming factors, 207  
 pharmacies, 539, 542–544  
 risk identification, 627  
 as robbery risk, 65  
 security training, 255  
 staff selection process, 377
- DSM, *see* Diagnostic and Statistical Manual  
 of Mental Disorders (DSM)
- Due diligence, in employee selection, 376–377
- Dummy cameras, 470–471
- Dupont, Lori, 491
- Duress alarms  
 definition, 452  
 employee security knowledge, 402  
 at front desk, 532  
 lockdown, 457  
 off-campus facilities, 571  
 pharmacies, 540–541  
 positioning, 638  
 as safeguards, 535  
 TJC standards, 98  
 usage, 452  
 workplace violence, 496–497

- Duress codes
  - pharmacies, 541
  - usage, 453
- Dustpan, patrol vehicle equipment, 284
- Duty belt, 225–226
- DVRs, *see* Digital video recorders (DVRs)
- E**
  - EAP, *see* Employee assistance program (EAP)
  - Earthquake emergency planning, 614, 592t
  - East Texas Medical Center, 621
  - EC, *see* Environment of Care (EC)
  - Ecoterrorism, 554–555
  - ED, *see* Emergency department (ED)
  - Education and training, *see also* Security officers, training
    - basic concepts, 233
    - conflict resolution, 644
    - department-specific programs, 396–397
    - ED staff, 537–539
    - employee programs, 394–397, 646
    - fire safety, 600–601
    - home caregivers, 568
    - infant security, 517f, 518f, 514–518, 514–515, 515–518, 644
    - instructors/facilitators, 258–259
    - materials, 259–261
    - security administrators, 162
    - security programs, 92–94
    - security sensitive areas, 507
    - security staffing, 149, 152
    - in shift supervision, 167
    - staff scheduling factors, 269
    - suggestions, 118–119
    - in supervision, 168–169
    - violence prevention, 496, 497–499
  - EEOC, *see* Equal Employment Opportunity Commission (EEOC)
  - 800 numbers, mass notifications, 478f
  - e-Learning, 259, 262
  - Elective training, 234, 255
  - Electromagnetic interference (EMI), 479
  - Electronic access control systems
    - after-hours, 456
    - considerations, 455
    - equipment carried, 219–221
    - importance, 637
    - intercoms/video door phones, 457–458
    - vs.* locks and keys, 430–431
    - managed, 458
    - technologies, 455t
  - Electronic card access
    - after-hours visitors, 356
    - building design, 106
    - gift shops, 559
    - ID badges, 383
    - parking control, 587
    - for patrol verification, 290–291
  - Electronic protected health information (EPHI), 15–16
  - Electronic reporting stations
    - vs.* daily activity report, 309
    - for patrol verification, 290
  - Electronic security safeguards and deployment patterns, 270
  - ED security, 535
  - infant abductions, 519–520, 644
  - security design, 636
  - security staffing, 153
  - wandering patients, 348–349
- Electronic security systems
  - alarms, 450–454
  - asset tracking, 475–479
  - central security station, 447–450
  - design considerations, 446–447
  - effectiveness, 641–642
  - emergency call boxes, 473–474
  - IAHSS guidelines, 443–444
  - implementation tips, 480–481
  - infant protection, 473, 520–521, 521t
  - lockdown, 456–457
  - mass notifications, 474–475
  - metal screening, 479
  - overview, 443
  - patients, 327
  - security master plan, 445–446
  - security sensitive areas, 456
  - testing, 480
  - video surveillance, 458–459
  - visitor management, 471–472
- Electronic signature capture pads, 471
- Electronic tagging
  - equipment, 437–438
  - infants, 473, 645
- Elements of Performance (EP)
  - SMP standards, 95, 97
  - TJC standards, 7, 10
- Elevator security
  - earlier years, 39t
  - fire safety, 599–600, 601
  - infant protection, 473, 520–521, 645
  - internal protection planning, 612
  - parking areas, 578
  - parking structures, 581
  - video surveillance, 462, 582–583
  - visiting hours, 355
  - wandering patients, 348–349
- Elopement, *see* Patient elopement
- EM, *see* Emergency Management (EM) Standard
- E-mail
  - employee education, 398–401
  - mass notifications, 475, 478f
- Embezzlement
  - investigation, 409–410
  - as security risk, 59
- Emergency announcement codes, 615–616
- Emergency call boxes
  - electronic security systems, 473–474
  - example, 475f
  - mass notifications, 478f
  - parking structures, 581–582
  - purpose, 640–641
- Emergency department (ED)
  - access control layout, 534f
  - after-hours visitors, 356
  - assessment, 530–531
  - combative patients, 339–340
  - compartmentalization, 533
  - deployment goals, 267–268
  - design considerations, 531–535
  - driveways/parking areas, 531
  - emergency signals, 539
  - example incidents, 527–539
  - family consult room, 534
  - forensic patients, 345
  - IAHSS guidelines, 529
  - interaction protocols, 536–537
  - metal screening, 479
  - officer training, 536
  - police interactions, 365
  - policy and procedures, 537
  - quiet/observation rooms, 533–534
  - safeguards, 535
  - safe room, 534–535
  - security master plan, 445
  - security/police room, 539
  - as security risk, 57–58
  - security sensitive areas, 505, 506
  - staff education, 537–539
  - staffing, 535–537
  - triage/front-desk, 532
  - video surveillance, 462
  - violence, 483–484
  - visitor control, 354, 537
  - waiting and admissions, 531–532
  - walk-in area, 531–532
- Emergency events
  - accidental and natural, 614–615
  - bombs and threats, 601–605
  - definition, 592–593
  - fire prevention and control, 597–601
  - fire safety programming, 597
  - IAHSS guidelines, 593–594
  - management phases, 594
  - primary manmade, 597–614
  - response times, 148, 150–151
  - security staffing, 616–617
- Emergency exit
  - civil disturbances, 612
  - patrolling, 278
  - robbery event, 65
  - signage, 423, 440–441
- Emergency Management (EM) Standard
  - removal from EC, 97
  - vs.* security management, 24
  - TJC, 35
- Emergency medical service (EMS)
  - bollards, 428
  - and linen loss, 553
  - pandemic events, 613
  - police interactions, 365
- Emergency message support, 126
- Emergency Nurses Association (ENA)
  - ED security, 529
  - security program influence, 35t
  - violence threats, 622
  - workplace violence, 483–484, 487–488, 642
- Emergency Operations Plan (EOP)
  - ICS, 596–597
  - management phases, 594
  - natural disasters, 614
  - pandemic events, 613
  - security staffing, 616–617
  - surge/lockdown, 616
  - TJC, 35
- Emergency planning
  - access control, 616, 617t
  - active shooters, 613–614
  - announcement codes, 615–616
  - biological/radiological weapons, 609–610
  - bombs and threats, 601–605
  - civil disturbances, 611–613
  - employee travel/housing, 618–619
  - event categories, 591–597
  - example situations, 592t
  - external protection, 611–612
  - federal government, 592–594
  - fire response, 601
  - gang/mob issues, 610–611
  - hospital leadership, 594
  - IAHSS, 592–594
  - ICS, 596–597
  - internal protection, 612–613
  - marked vehicles, 618
  - mutual aid, 617–618
  - NIMS funding, 597
  - pandemic events, 613
  - security uniforms, 618
  - strikes and picketing, 605–608
  - terrorism, 608–610
  - TJC, 592–594
  - WMDs, 609
- Emergency preparedness
  - director position, 594
  - drills, 594–596
  - overview, 591
  - responsible positions, 595t
  - security training, 254–255
- Emergency response time, staffing considerations, 150f, 150–151
- Emergency shipment support, 127

- Emergency signals, ED training, 539  
 EMI, *see* Electromagnetic interference (EMI)  
 Empathy  
   officer traits, 184f  
   RATER model, 245  
 Employee assistance program (EAP), 391  
 Employee entry points  
   access control, 541  
   central security station, 449  
   CPTED security principle, 583f  
   security master plan, 445, 445  
 Employee health record release, 367, 370  
 Employee informants, 420–421  
 Employee issues  
   accident reporting, 117–118  
   accident risk, 71  
   activist infiltrations, 555  
   background checks, *see* Background checks  
   business office/cashier risks, 557  
   emergency messages, 126  
   emergency travel/housing, 618–619  
   fire event reactions, 600  
   fire safety training, 600–601  
   nonstriking, 606  
   off-duty, 385  
   officer referral programs, 181f  
   parking options, 586, 586  
   perceived officer role, 180  
   performance documentation, 173  
   performance management, 173  
   picket lines, 606–607  
   police interaction, 364–371  
   problem employees, 176  
   protection program role, 105, 645–646  
   relations with, 130  
   research labs, 555  
   security reporting, 447  
   security responsibility, 385  
   time recording, 390  
   weapons policy, 385–386  
 Employee lockers  
   access control, 122  
   as psychological deterrents, 31  
   security policies, 388–389  
   stolen property, 31  
 Employee property  
   losses, 70–71  
   package check, 127  
   security education, 92  
 Employee security education  
   crime prevention, 397, 397–401  
   department-specific, 396–397  
   employee awareness, 397–401  
   handbill example, 401f  
   handouts, 400f, 398  
   IAHSS guidelines, 395  
   importance, 394–397  
   meetings, 401  
   newsletters, 397–398, 398f  
   personal safety, 397  
   presentation and handouts, 394–396  
   websites/e-mail, 398–401  
 Employee security knowledge  
   crime triangle, 403–404  
   customer service greetings, 403  
   escorts, 403  
   incident reporting, 402–403  
   safety perception, 404–405  
 Employee selection  
   applicant suitability, 377–378  
   via due diligence, 376–377  
   and HR office location, 375–376  
   as security issue, 377  
 Employee surveys  
   attitudes, 404–405  
   security initiatives, 399  
 Employee theft  
   controls on, 69  
   employee property loss, 70–71  
   facility property losses, 69  
   factors, 68–69  
   overview, 67–71  
   patient property loss, 69–70  
 Employee violence  
   considerations, 490–491  
   definition, 484  
 Employment guidelines, security-oriented  
   contraband, 390–391  
   drug testing, 391  
   EAP, 391  
   employee security responsibility, 385  
   employee time-recording, 390  
   investigation cooperation, 388  
   off-duty employees, 385  
   overview, 384–392  
   package inspection, 386–388  
   patient/family gifts, 389  
   staff lockers, 388–389  
   staff property loss, 391–392  
   staff solicitation/product distribution, 389  
   surplus/damaged property, 390  
   weapons policy, 385–386  
 EMS, *see* Emergency medical service (EMS)  
 ENA, *see* Emergency Nurses Association (ENA)  
 Engineering control room monitoring, 469  
 Engineering failure, 48  
 Entrance security  
   access control, 121, 277, 455, 534f, 541, 570, 637  
   after-hours access, 355, 456  
   automated controls, 587  
   bollards, 428  
   bomb threats, 55  
   central security station, 449  
   civil disturbances, 611–612  
   CPTED security principle, 583f  
   customer service, 111  
   ED security, 533, 534f  
   during emergencies, 99  
   external patrol, 278  
   HR department, 376f  
   infant security, 520f  
   large acreage facilities, 357  
   late night-shift employees, 586  
   lighting, 430f  
   lockdown, 457, 616  
   package inspection, 386  
   parking areas, 531  
   parking control, 577–578  
   parking structures, 580–581, 582  
   patrolling, 277  
   picket lines, 606–607  
   security design, 531  
   security master plan, 445  
   security response, 523–524  
   signage, 440  
   use policies, 30  
   video door phones, 457  
   video surveillance, 460, 462, 519, 582–583  
   visitor contact, 353  
 Environmental criminology, definition, 75  
 Environment of Care (EC)  
   components, 10–11  
   EM removal, 97  
   healthcare executive primer, 621  
   monthly/periodic reports, 312–313  
   security incident statistics, 304  
   security risk assessment, 77  
   TJC time line, 37f  
   U.S. hospital security history, 24  
 EOP, *see* Emergency Operations Plan (EOP)  
 EP, *see* Elements of Performance (EP)  
 Equal Employment Opportunity  
   Commission (EEOC), 378–379  
 Equipment carried  
   basic considerations, 215–226  
   batons, 224  
   chemical agents, 221–224  
   communication devices, 216–217  
   duty belt, 225–226  
   flashlight, 218  
   handcuffs, 217–218  
   notepad and pen, 215  
   patrol vehicle, 283–284  
   PPE, 218–219  
   proper training, 227  
   protective vests, 224–225  
   radios, 640  
   Tasers, 219–221  
   use of force training, 243–244  
 Equipment rooms  
   access control, 121  
   bomb threat prevention, 602  
   internal protection planning, 612  
 Equipment and supplies  
   accountability and marking, 551  
   as burglary target, 56  
   distribution, 128, 551  
   emergency shipments, 127  
   employee theft, 67  
   fastening down, 437–438  
   firearms, 206–226  
   inspection policies, 386–388  
   open-view removal, 387  
   theft risk, 67  
   video surveillance, 463–468  
 ESC, *see* Evidence of Standards Compliance (ESC)  
 Ethical behavior, obstacles, 164  
 Ethical standards  
   officer performance, 191f  
   security leadership, 163–164  
 Euphoric response, wandering patients, 348  
 Evacuation  
   bomb threat plan, 604  
   fire safety program, 599–600  
   mass notifications, 478f  
 Event-driven monitoring  
   benefits, 639  
   CCTV, 460  
 Evidence of Standards Compliance (ESC), 9  
 Exempla Saint Joseph Hospital (CO), 354–355  
 Exit security  
   access control, 616, 617f  
   after hours access, 355  
   automated control, 587  
   blocked exits, 287  
   civil disturbances, 612  
   compartmentalization design, 533  
   CPTED principle, 583f  
   external patrol, 278  
   fires, 598–599  
   infant security, 473, 519, 520f  
   internal protection planning, 612  
   lockdown, 457, 616  
   package inspection, 386  
   parking control, 578  
   parking structures, 581, 582  
   patrolling, 266, 277–278, 277, 278  
   picket lines, 606–607  
   robbery event, 65  
   seals, 436  
   security design, 531  
   signage, 423, 440–441  
   traffic flow, 587  
   triage, 532  
   video surveillance, 520f, 571, 582–583  
   wandering patients, 348–349  
   workplace violence, 498  
 Explosions, 59, 120  
 Extended workforce, as security loophole, 380

- External audits
  - overview, 123–124
  - testing, 123–124
- External emergencies
  - reaction to, 119–120
  - as safety risks, 72
- External motivations, psychological
  - deterrents, 29–30
- External patrol
  - area crime, 151
  - battery-jumping service, 282–284
  - entrances/exits, 277
  - function, 277–278
  - officer arming, 213
  - post assignments, 272
  - scheduling, 270
  - services, 282
  - transporting people, 283
  - uniforms, 203
- External patrol vehicles
  - advantages/disadvantages, 278–282, 279f
  - basic considerations, 278–279
  - bicycle patrol, 280–281
  - damage, 284
  - equipment, 283–284
  - inspection report, 285f
  - operation, 284
  - personal transporters, 281–282
  - security carts, 280
  - transporting people, 283
- External security factors
  - ASIS International, 41
  - CMS, 38
  - IAHSS, 38–42, 39t
  - The Joint Commission, 35–36
  - legislation, 42–43
  - NCMEC, 36–38
  - NFPA, 41–42
  - non-U.S. countries, 43–45
  - ordinances, 42–43
  - OSHA, 38
  - security programs, 35t
  - State Health Department, 42–43
- Eye contact, in customer service, 111
- F**
- Face-to-face debriefing, undercover
  - operatives, 419–420
- Facial recognition software, 354–355
- Facilitators, training resources, 258–259
- Facility orders, definition, 296–297
- Fairchild Air Force Hospital (WA), workplace
  - violence, 485
- Fair Credit Reporting Act (FCRA)
  - background checks, 378–379
  - and investigations, 408
- Fair Labor Standards Act (FLSA), uniform
  - regulations, 204
- Fake cameras, video surveillance, 470–471
- False alarms
  - handling, 453–454
  - video analytics, 467
- False sense of security, *vs.* behavior
  - inhibition, 31–32
- Family abductions
  - basic problem, 527
  - issues, 527
  - protection strategies, 528t
- Family consult room security, 534
- Farnham Road Hospital (UK), 324–325
- FBI counterintelligence domain project, 362
- FCRA, *see* Fair Credit Reporting Act (FCRA)
- Federal Animal Enterprise Protection Act, 555
- Federal Emergency Management Agency
  - (FEMA), 254–255
- Federal Privacy Act, 378–379
- Federal Trade Commission (FTC)
  - FCRA, 408
  - identity theft risks, 61
  - IT security, 558
- Female security officers, 184
- Fencing
  - chain link, 426
  - decorative metal fencing, 426–427
  - example, 427f, 427f
  - as physical safeguard, 424–427
  - as psychological deterrence, 32
  - security layering, 424
  - surface parking lots, 579–580
  - wage compensation, 189
- Fentanyl abuse/theft, 58, 543
- Fingernail polish remover, prescription
  - altering, 544
- Fingerprint readers, 471, 543–544
- Firearms
  - arming considerations, 206–213
  - arming trends, 213
  - and community standard, 211–212
  - deterrent value, 208
  - environmental profile, 208–211
  - liability, 207–208
  - officer affidavit training, 214f
  - officer disarming, 212
  - personal safety, 207
  - personnel quality, 212
  - policies, 213–215
  - usage, 206–226
  - as use of force, 636
  - vulnerability, 207
  - weapon/holster/ammunition, 212–213
  - weapons experience, 211
- Fire department
  - security liaison, 372–373
  - security staffing, 148
  - vs.* standard of care, 48
- Fire events
  - emergency preparedness, 592t
  - employee reaction, 600
  - prevention and control, 597–601
  - as security concern, 120
  - security response, 601
  - as security risk, 59
- Fire extinguisher
  - fire safety, 600
  - informational signs, 440
  - internal patrol, 287
  - internal protection, 612
  - patrol vehicle equipment, 283
  - performance evaluations, 187t
  - training program, 261
  - types, 600
- Fire safe, 439
- Fire safety program
  - containment, 598–599
  - detection, 598
  - elements, 597
  - evacuation, 599–600
  - extinguishment, 600
  - prevention, 598
  - training, 600–601
- Fire watch, U.S. hospital security history,
  - 22–23
- First-aid kit, patrol vehicle equipment, 284
- First patrol, importance, 288
- “Fishing expedition” surveillance, 416
- Fixed-post assignments
  - as deployment issue, 265
  - function, 271
  - planned, 152
  - problems, 294
  - reading during, 294
  - safeguard-risk matching, 80
  - security staffing, 148, 150f, 152
- Flag etiquette, 128
- Flammable liquids, glazed glass protection,
  - 436
- Flares, patrol vehicle equipment, 284
- Flashlight
  - equipment carried, 218
  - patrol vehicle equipment, 284
- Flex cuffs, equipment carried, 217
- Flexing staffing plan, 266–267
- Flood emergency planning, 120, 614, 592t
- FLSA, *see* Fair Labor Standards Act (FLSA)
- Follow-up investigations
  - incident investigation phases, 412
  - preliminary relationship, 413
- Food service security, 561
- Footprints, infant identification, 513
- Forensic patients
  - delivery training, 254
  - IAHSS guidelines, 347
  - management, 645
  - protocol, 349f
  - security involvement, 344–348
- Foreseeability, security risk assessment, 75
- Forged prescriptions, 544
- For Healthcare Professionals: Guidelines on Prevention of and Response to Infant Abductions*, 509, 514
- For Hospital Professionals: Guidelines on Preventing Abduction of Infants from Hospital*, 509
- For-profit hospitals, 3–4
- Foundations for Action*, 393
- Four-band identification system, 513
- Fraternization issues, 141
- Fraud
  - audits, 123
  - cash/payment handling, 575
  - cash registers, 126
  - employee informants, 420–421
  - employee selection process, 377
  - employee time recording, 390
  - gifting issues, 389
  - investigations, 409–410, 416
  - police misrepresentation, 363–364
  - property distribution, 551
  - purchasing and receiving, 549
  - security risks, 53f, 62–63
  - vendor fraud, 63
- Fringe benefits, security staffing, 149, 153
- Front-desk reception, ED security, 532
- FTC, *see* Federal Trade Commission (FTC)
- FTE, *see* Full-time equivalent (FTE)
- Fuel dispensers, fencing security, 426
- Full-time equivalent (FTE)
  - deployment, 265
  - and flexing, 266
  - officers, 188
  - security department organization, 133
  - security staffing, 90, 157, 629–630
- Full-time security officers, 187–189
- Funding overview, 34, 597
- G**
- Gang issues
  - emergency planning, 610–611
  - emergency preparedness, 592t
  - ICU security, 559
  - security training, 252–253
- Garbage inspection, activist infiltrations, 555
- Garcia v. Bronx Lebanon Hospital*, 226
- Garden fencing, 427f
- Gasoline dispenser fencing, 426
- General nursing unit, combative patients,
  - 338–339, 341
- Geography, in healthcare delivery, 2–3
- Geriatric units

- and intermediate care, 3
  - risk assessment, 80f
  - video surveillance, 462
  - workplace violence, 483–484, 485
  - “Giant Voice,” mass notifications, 478f
  - Gifts, from patients/family, 389
  - Gift shops
    - alarms, 638
    - security concerns, 559
  - Glazing safeguards
    - bullet resistive glass, 437, 535, 541
    - civil disturbances, 611–612
    - ED access control, 534f
    - glass protection, 436–437
    - parking control, 588
    - parking structures, 580, 581, 582
    - as physical deterrent, 28t
  - Global Positioning Systems (GPS)
    - communication devices, 216
    - home caregivers, 565, 568
  - Gloves, as PPE, 218
  - Golan, David, 527–528
  - Government agency liaisons, 122–123
  - Government hospitals, definition, 3
  - Grand jury subpoenas, 368, 370
  - “Green” alternatives, bicycle patrols as, 281
  - Grounds lighting, selection and design, 428–429
  - Group behavior, communication issues, 168
- H**
- Hallcrest Report II, 359–360
  - Hampton, Richard, 483
  - Handbill notices
    - employee education, 398
    - example, 401f
  - Handcuffs
    - equipment carried, 217–218
    - forensic patients, 346
    - as use of force, 636
  - Hand lanterns, patrol vehicle equipment, 284
  - Handouts
    - employee education, 398
    - example, 399f, 400f
  - Hand-written reports, typing, 306
  - Hard data goals, security staffing, 150–152
  - Harmful behavior, ED training, 538
  - Hazard communications, OSHA compliance, 246
  - Hazard vulnerability analysis (HVA)
    - definition, 51
    - emergency planning, 591–592
  - HCFs, *see* Healthcare facilities (HCFs)
    - security guidelines
  - HCOs, *see* Healthcare Organizations (HCOs)
  - Healing environment overview, 19
  - Healthcare categories, definitions, 2–3
  - Healthcare environment basics
    - challenges, 1
    - CMS overview, 15–16
    - cost growth, 2
    - cost inefficiencies, 2
    - facility staffing, 5–6
    - HIPAA overview, 14–15
    - hospital types, 3–4
    - nonhospital side, 4–5
    - physician role, 6–7
    - post-9/11 safety concerns, 1
    - safeguarding responsibilities, 1
    - security administrator, 7
    - stakeholders, 5
    - TJC overview, 7–14
  - Healthcare facility (HCFs) security guidelines
    - access control-identification system, 381–382
    - CCTV, 459
    - covert investigations, 418–419
    - design, 44
    - electronic security systems, 443–444
    - emergency care, 529
    - emergency management, 593–594
    - forensic patients, 347
    - general staff security orientation, 395
    - home health security, 565
    - industry guidelines, 40
    - infant/pediatric security, 512
    - investigations, 410–411
    - officer training, 233–234
    - patient elopement, 328
    - primary security risks, 52–72
    - searching patients, 333
    - security design, 636–637
    - security incident reporting, 302
    - security management plan, 86
    - security-patient relationship, 317
    - security program measurement, 96
    - security risk assessment, 82
    - security sensitive areas, 506
    - targeted violence, 501–502
    - use of force, 226–227
    - workplace violence, 493–494
  - Health Care Financing Administration, *see* Centers for Medicare and Medicaid Services (CMS)
  - Healthcare industry staffing, 5–6
  - Healthcare management process, 9f
  - Healthcare Organizations (HCOs), 40
  - Healthcare Security Council, 160
  - Healthcare systems, security organization
    - chart, 136f, 135–136
  - Health information management (HIM),
    - basic considerations, 547–556
  - Health Information Technology for Economic and Clinical Health (HITECH) Act, 558
  - Health Insurance Portability and Accountability Act (HIPAA)
    - CMS guidelines, 15–16
    - forensic patient delivery, 254
    - information management, 548
    - overview, 14–15
    - requests for information, 366–367
    - security administration, 7
    - security effectiveness, 443
    - security program objectives, 624
    - video surveillance recording, 468
  - Health Resources and Services Administration (HRSA), 597
  - Health Revolutionary Unity Movement, 610–611
  - Heating, ventilation, and air conditioning (HVAC) system, 222–224
  - HEICS, *see* Hospital Emergency Incident Command System (HEICS)
  - Helpfulness, officer traits, 184f
  - Hemphill, Barbara, 295
  - Henry Ford Medical Center (MI), 211, 492
  - Hepatitis-B, security problems, 338
  - Hertig, Christopher, 233
  - Heskett, Sandra L., 485
  - HICS, *see* Hospital Incident Command System (HICS)
  - HIM, *see* Health information management (HIM)
  - HIPAA, *see* Health Insurance Portability and Accountability Act (HIPAA)
  - Hiring process
    - administrator issues, 159–160
    - background checks, 378–379, 380, *see also* Background checks
    - due diligence-based selection, 377
    - and HR, 375–376
    - licensing requirements, 178–179
    - management selection, 163
    - negligent hiring, 119, 377
    - recruitment, 180
    - security administrators, 625
    - security role, 380–381
    - selection criteria, 183
    - vendor employees, 550
    - workplace violence prevention, 494
  - HITECH, *see* Health Information Technology for Economic and Clinical Health (HITECH) Act
  - HIV, *see* Human immunodeficiency virus (HIV)
  - H1N1 Influenza A virus, 613
  - Holdup alarm
    - pharmacies, 540–541
    - usage, 452
  - Holidays
    - animal activist infiltrations, 556
    - deployment plans, 276
    - security e-mail broadcasts, 399–401
    - security handouts, 400f
  - Holster, arming officers, 212–213
  - Home care, definition, 3
  - Home healthcare provider
    - assaults to, 65
    - caregiver at risk, 566–567
    - IAHSS security guidelines, 565
    - as off-campus service, 564–568
    - patient at risk, 566
    - security practices/guidelines, 567–568
    - security strategies, 569t
  - Homeland Security, DoD role, 608–609
  - Homeland Security Exercise and Evaluation Program (HSEEP), 595
  - Home purchase assistance, as community outreach, 103
  - Home safety, security education, 119
  - Homicide
    - ICUs, 559
    - incident increase, 19, 622
    - inpatients, 320
    - officer negligence, 177
    - as security risk, 60–61
    - security risks/vulnerabilities, 53f
    - threat assessment, 81f
    - as TJC sentinel event, 13f, 12, 326
    - workplace violence, 485, 642
  - Hospital Emergency Incident Command System (HEICS), 596
  - Hospital Emergency Preparedness Manuals,
    - new officer training, 241
  - Hospital Incident Command System (HICS), 596
  - Hospitalist position, 586
  - Hospital Policy Manual, new officer training, 241
  - Hospital Safety and Security Act, workplace violence, 499
  - Hospital security basics
    - as healthcare security basis, 22
    - history, 22–25
  - Hospital types, definitions, 3–4
  - Hospital watch, definition, 405–406
  - Hostage taking
    - critical incident response plan, 507–508
    - as security risk, 53f, 66, 59–60
  - Hotel-Dieu Grace Hospital (Canada),
    - workplace violence, 491
  - House detective, definition, 22
  - Housing, emergency planning, 618–619
  - HPE, *see* Human performance evaluation (HPE)
  - HR, *see* Human Resources (HR) department
  - HRSA, *see* Health Resources and Services Administration (HRSA)
  - HSS Inc., shared central security station, 449–450



- Human immunodeficiency virus (HIV), security problems, 336–338
- Human performance evaluation (HPE) officer selection process, 187 sample measurements, 187t
- Human Resources (HR) department applicant background investigation, 119, 378–379 applicant information, 379 applicant suitability, 377–378 application forms, 377–378 background screening providers, 379–380 department-specific security training, 396 employee health records, 367 employee security responsibility, 385 employee selection, 377 extended workforce loophole, 380 ID badge administration, 382–383 ID badge design, 383–384 ID badge guidelines, 381–382 ID badge overview, 381–384 investigation cooperation, 388 off-duty employees, 385 office location, 375–376, 376f package inspection policies, 386–388 police interactions, 364 responsibilities, 375 security in hiring, 380–381 security master plan, 445 security-oriented issues, 384–392 staff locker policy, 388–389 staff selection, 376–377 staff solicitation/product distribution, 389 weapons policy, 385–386 workplace violence, 492
- Hurricane Katrina, 24, 592–593
- Hurricane Rita, 592–593
- Hurricanes, 478f, 614, 592t
- HVA, *see* Hazard vulnerability analysis (HVA)
- HVAC, *see* Heating, ventilation, and air conditioning (HVAC) system
- I**
- IAHSS, *see* International Association for Healthcare Security and Safety (IAHSS)
- ICS, *see* Incident Command System (ICS)
- ICUs, *see* Intensive Care Units (ICUs)
- Identification badges administration, 382–383 after-hours visitors, 356 design, 383–384 emergency planning, 618–619 IAHSS guidelines, 381–382 infant security, 514 IT security, 558 overview, 381–384 uniform styles, 202 visiting hours control, 354–355 visitor management, 640
- Identification bracelets, 513–527
- Identity theft executive primer, 627 officer training, 248t security education, 119 as security risk, 61
- IESNA, *see* Illuminating Engineering Society of North America (IESNA)
- Illegitimate visitors as perpetrator, 487 security patrols, 30–31 workplace violence, 489, 496, 489–490
- Illuminating Engineering Society of North America (IESNA), 580–581
- Image factor in officer selection, 183 security principles, 194f in staff scheduling, 269
- Imposters as security risks, 53f, 62 security risks/vulnerabilities, 627 staff education, 514–515 TJC surveyors, 472
- Inappropriate behavior autistic patients, 344 security coordination, 102
- Inattentiveness, as security issue, 403–404
- Incapacitation, as use of force, 635t
- Incident Command System (ICS) bomb threats, 602 as EOP component, 596–597 FEMA training, 254–255
- Incident reports employee security knowledge, 402–403 and risk assessment, 267 violence prevention, 496
- Incident response plan infant abductions, 522–525 security sensitive areas, 507–508
- Industry Standard of Practice (ISP) best practices, 47 definition, 46–47 ED compartmentalization, 533 policy and procedures, 297 video recording, 468
- Infant abductions abductor methods, 511–512 abductor profile, 511–512 access control, 519 alarm reduction strategies, 521t concerns, 644–645 as contemporary issue, 252 critical incident response plan, 507–508, 522–525 discharge issues, 525–527 drills and exercises, 526f, 525, 621 electronic monitoring, 520–521 emergency announcement codes, 615 employee response, 396 facility-wide staff response, 523 family abductions, 527, 528t fire prevention and control, 597 from HCFs, 508–512 hospital infant environment, 511 IAHSS guidelines, 512 industry standard practice, 46–47 infant identification, 513–527 media relations, 524–525 new employee training, 242f by nonfamily members, 509t parental education, 517f, 518f, 515–518 precautions/guidelines, 521–522 prevention, 514–518, 644 prevention/response, 94, 647t protection systems, 473 response training, 118 risks, 63, 350–351 security drills, 98 security effectiveness, 443 security plan basics, 512 security risks/vulnerabilities, 627 security safeguards, 519–520 security staff response, 523–524 security training, 633t sensitive areas, 506 specialized training, 255 staff education, 514–515, 515t state statistics, 510t switching as problem, 71 tagging, 645 as TJC sentinel event, 12, 97 treatment room access, 120 unit nursing personnel, 522 video surveillance, 519–520, 520t vulnerable areas, 527
- Infant monitoring systems basic considerations, 520–521 reduction strategies, 521t
- Infectious patient security, 336–338
- Infiltration issues animal activist methods, 555–556 undercover investigations, 418
- Informants, employee, 420–421
- Information department security, 506
- Information loss via misuse, 71 as security risk, 64
- Information release guidelines employee health records, 367 exchange issues, 296 grand jury subpoena, 368 key considerations, 370–371 overview, 367–368 patient medical records, 367, 369 personnel records, 368, 368–369 privileged communication, 368 public safety liaison, 366–367 pursuant to search warrants/subpoenas, 370 search warrants, 368
- Information storage room control, 120
- Information technology (IT) IP cameras, 464 security concerns, 557–559 security master plan, 445 systems integration, 444
- Infrared (IR) vs. IP cameras, 466
- In-house security staff, *see also* Proprietary security staff applicant quality, 145 bulletins, 261 characteristics, 138–139 with contract staff, 142 during emergencies, 617 equipment maintenance, 105 ID badges, 383–384 as instructors, 259 vs. outsourcing, 139–140 qualifications, 73 recruitment issues, 180 security history, 23 sentinel event processing, 13–14 small facilities, 157 as staff model, 139, 138t as staff type, 136 supplemental training, 251 training formats, 248–249 training funds, 233 work shift, 269–270
- In-house surveys bomb search, 603 emergency conditions, 617 employee attitudes, 405
- Initial investigation, *see* Preliminary investigation
- Inpatient assistance, *see* Patient care involvement
- In-service education departments, department-specific security training, 396
- Inside job, activist infiltrations, 555
- Inspections external audits, 123–124 garbage by activist groups, 555 patrol vehicles, 285f sample report, 170f trash collection systems, 287
- Instructors, security training, 232, 258–259
- Integrity tests, officer selection process, 186
- Intensive Care Units (ICUs) combative patients, 340–341 infant abductions, 510–511 maintaining order, 111–112

- security concerns, 559
- security sensitive areas, 505
- visiting hours, 354
- visitor control, 354
- Interchangeable core lock design, 432
- Intercom systems
  - access control, 457–458
  - emergency call boxes, 473–474
  - mass notifications, 478f
  - with video, 468, 469, 535
- Intermediate care, definition, 3
- Internal audits, 123–124
- Internal emergencies
  - preparation for, 591
  - reaction to, 119–120
  - as safety risks, 72
- Internal patrols
  - vs.* external, 278
  - fixed posts, 152
  - operational *vs.* nonoperational times, 275
  - purpose, 286–287
- Internal security factors
  - corporate policy, 34–35
  - funding, 34
  - leadership, 33–34
  - organization philosophy/culture, 33
- International Association for Healthcare Security and Safety (IAHSS)
  - Canada, 44
  - CCTV guidelines, 459
  - cover investigation guidelines, 418–419
  - ED security, 529
  - electronic security systems, 443–444
  - emergency management, 593–594
  - emergency planning, 592–594
  - forensic patient security, 347
  - home health security, 565
  - identification system guidelines, 381–382
  - infant abductions, 522
  - infant/pediatric security, 512
  - investigation guidelines, 410–411
  - officer ethics, 191f
  - officer recruitment, 182
  - officer training, 233–234
  - patient care involvement, 317
  - patient elopement guidelines, 328
  - patient search guidelines, 333
  - required reading, 160
  - risk assessment, 73, 74–75
  - security administrators, 88, 625
  - security guidelines, 39t, 82–83
  - security programs, 38–42, 624
  - security sensitive areas, 506
  - security staffing, 147–149
  - seminars, 162
  - SIR guidelines, 302
  - SMP guidelines, 86, 96–97, 94–95
  - staff security education, 395, 397
  - targeted violence, 501–502
  - training certification, 632
  - training guidelines, 231–232
  - training record standards, 262
  - use of force guidelines, 226–227
  - wage compensation, 189
  - workplace violence, 493–494
- International Association for Healthcare Security and Safety (IAHSS) Progressive Certification
  - Advanced Training, 249–250, 250t
  - basic elements, 258t
  - Basic Training, 247–249, 248t
  - definition, 234
  - overview, 246–250
  - Supervisory Training, 250–251, 251t
- International Organization for Standardization (ISO), 41
- Internet recruitment resources, 182
- Interrogation techniques, 417–418
- Interviewing techniques, 417–418
- Intoxication
  - patient elopement, 325–326
  - as security risk, 58
  - security watch, 329
  - Taser use, 222f
- Introduction to ICS (IS-100)*, 254–255
- Intruders
  - alarm deterrents, 451
  - animal activists, 556
  - entrances/exits, 277
  - hiding in landscaping, 427
  - pharmacies, 542
  - security condition report, 307
  - thermal imaging cameras, 467
  - video analytics, 466
  - video surveillance, 458, 639
  - workplace violence, 487
- Intrusion alarm
  - gift shops, 559
  - pharmacies, 542
  - positioning, 638
  - usage, 452
- Inventorying locks and keys, 436
- Investigations, *see also* Background checks
  - audit overview, 415
  - background check overview, 414–415
  - cooperation with, 388
  - data collection, 112–113
  - employee informants, 420–421
  - and FCRA, 408
  - IAHSS guidelines, 410–411
  - inadequate, 413–414
  - incident investigation, 411–416
  - interviewing/interrogation, 417–418
  - investigator attributes, 416–417
  - minor crimes, 409
  - nonincident-driven, 414–416
  - personnel records release, 368–369
  - phases, 411–416
  - vs.* police investigations, 408–409
  - preliminary-follow-up relationship, 413
  - as psychological security deterrent, 32
  - reasons for, 407–408
  - as security component, 407
  - spot checks/surveillance, 415–416
  - style, 407
  - in systems security programs, 145
  - types, 409–410
  - undercover, 418–420
  - wrongdoing/suspect patterns, 414
- Investigative report, *see* Security incident report (SIR)
- Investigators
  - attributes, 416–417, 417t
  - on investigative loan, 419–420
  - outside, 409–410
- Iowa Methodist Medical Center, infant security, 516
- IP cameras, 464–466
- IR *vs.* IP cameras, 466
- Irrational behavior, general nursing unit, 341
- Islandism, definition, 144
- ISO, *see* International Organization for Standardization (ISO)
- Isolation unit control, 354
- ISP, *see* Industry Standard of Practice (ISP)
- IT, *see* Information technology (IT)
- J**
- Jacobs, George, 168
- JCI, *see* Joint Commission International (JCI)
- JCR, *see* Joint Commission Resource (JCR)
- Jeffery, C. Ray, 441
- Job fair recruitment, 182
- Job promotion
  - contract staff, 140–141
  - due diligence-based, 377
  - leadership development, 255–256
  - performance expectations, 191
  - security supervisors, 166
- Job satisfaction, 68, 185
- Job status, officers, 109f
- Johns Hopkins Hospital (MD), 281, 319
- Joint Commission on Accreditation of Hospitals (JCAH), 7
- Joint Commission International (JCI), 8
- Joint Commission Resource (JCR), 8
- Journal of Healthcare Protection Management*, 162
- Jumper cables, 284
- “Just in time” delivery, 549
- K**
- Kending, Jim, 346–347
- Kent Hospital (RI), 280–281
- Keys, *see also* Locks and keys
  - and access control, 121
  - computer-based key accountability, 433–434
  - employee locker access, 122
  - handcuffs, 218
  - making, 435
  - and pass-on record, 311–312
  - patrol officer, 291–292
- Kickbacks
  - purchasing and receiving, 549
  - security investigations, 409–410
  - as security risk, 53f, 62–63
- Kidnapping risk, 53f, 66, 63
- King Henry VIII, 22
- Kings County Hospital (NY), 338
- Knowles, Malcome, 232
- Knox-Box key system, 561
- L**
- Labor action risks, 63–64
- Labor management software, 269
- Laissez faire* management, 141–142
- Lancaster General Hospital (PA), 469
- Landscaping
  - external protection planning, 611–612
  - fencing appearance, 427
  - tree/shrub barriers, 429–430
- Large acreage facility control, 319
- Late night-shift employee parking, 586
- Laundry
  - access controls, 554
  - alarms, 638
  - control, 552
  - scrubs losses, 553–554
- Law enforcement agencies
  - vs.* administrative remedy, 20–21
  - arming liabilities, 207
  - contact frequency, 371–372
  - criminal justice interface, 104
  - ED security staffing, 535–536
  - emergency planning, 618–619
  - emergency room activity, 365
  - forensic patients, 346–347, 645
  - vs.* health care security, 20, 20t
  - information exchange, 296
  - information release, 367
  - investigation purpose, 407
  - liason with, 122–123
  - lockdown capability development, 457
  - off-duty, *see* Off-duty law enforcement officer recruitment, 182
  - public safety coordination, 103
  - security liason, 359–361, 372t

- Law enforcement agencies (*continued*)  
 service requests, 362–364  
 U.S. hospital security history, 23  
 violence prevention, 497
- Leadership development  
 competencies, 257–258  
 definitions, 256–257  
 overview, 255–258  
 personnel effectiveness, 234–235  
 security administrators, 625–626  
 security training, 631  
 success traits, 257t
- Leadership responsibilities  
 officer competency verification, 240  
 security programs, 33–34  
 security supervisors, 164–172  
 SMP, 87
- LEAPS, *see* Dallas/North Texas Regional Law Enforcement and Security Program (LEAPS)
- Learning management software (LMS), 262
- Leather duty belt, 225
- Legislation  
 APPL, 361  
 background checks, 555  
 community programs, 371  
 emergency preparedness, 595  
 employee weapons, 386  
 infant security, 509  
 licensing laws, 179  
 neighborhood stability, 103  
 officer retention, 299  
 officer selection criteria, 183  
 polygraph tests, 186  
 security influence, 35t  
 security program factors, 42–43  
 signage, 439–440  
 workplace safety, 88–89  
 workplace violence, 499–500, 500
- Liability issues  
 arming officers, 207–208  
 canine patrols, 286  
 documentation policies, 299  
 electronic security, 443, 480  
 extended workforce, 380  
 external audits, 124  
 FCRA, 408  
 firearms, 206  
 IAHS training guidelines, 248t, 250t, 251t  
 inadequate training, 235  
 infant monitoring, 521  
 information release, 370–371  
 investigations, 407  
 IP cameras, 464  
 locks and keys, 430–431  
 outsourced security, 557  
 patient management, 21  
 patient property loss, 70  
 personnel records, 368–369  
 restraint training, 244  
 risk management, 26  
 security rationale, 21  
 security technology, 641–642  
 from Taser use, 221  
 training importance, 234–235, 631  
 use of force, 221, 636  
 video surveillance, 584  
 weapons, 213
- Library access control, 121, 638
- Licensed practical nurse (LPN), imposters, 62
- Licensing issues  
 child development centers, 556–557  
 NFPA, 41–42  
 non-U.S., 43  
 officers, 178–179  
 officer selection, 185  
 security rationale, 21  
 staff scheduling factors, 269
- State Health Department, 42  
 tracking software, 269  
 uniform styles, 202–203  
 weapons, 212–213
- Life Safety Code, 599–600
- Life safety-focused doors, 445
- Lighting  
 characteristics, 429t  
 external protection planning, 611–612  
 inspection, 123–124  
 off-campus facilities, 572–573  
 parking structures, 580–581  
 pharmacies, 542  
 as safeguard, 27, 428–429  
 security layering, 424  
 security standards, 430f  
 surface parking lots, 579–580  
 video analytics, 467
- Linens  
 control, 552  
 loss control, 553  
 loss figures, 552–554  
 marking, 554
- Line positions, as staffing category, 149–150
- Line supervisors, 159
- Listening skills, 498
- Litigation risk  
 background checks, 380  
 body of knowledge, 46  
 documentation policy, 174, 299  
 firearms training, 215  
 health information, 548  
 inadequate investigations, 413–414  
 parking areas, 578  
 records retention, 314–315  
 risk assessment, 76  
 security training, 631  
 signage, 441  
 special police commission, 177  
 Tasers, 221  
 as training motivation, 232, 631  
 use of force, 636  
 visitor accidents, 26
- Live monitoring  
 cost effectiveness, 639  
 full *vs.* none, 468–469  
 and response capability, 584  
 safeguard impacts, 153  
 video *vs.* alarms, 460  
 video surveillance, 458, 519
- LMS, *see* Learning management software (LMS)
- Lobby security  
 appropriate uniforms, 199–200  
 central security station, 449  
 CPTED security principle, 583f  
 field report writing, 301  
 missing patients, 322  
 post assignments, 272  
 as security risk, 57  
 video surveillance, 466, 582–583  
 visitor management, 640
- Local Security Management Specialist (LSMS), 88–89
- Lockdown  
 access control stages, 617t  
 considerations, 456–457  
 EOP, 616  
 importance, 638
- Locked area access control, 121–122
- Locker rooms  
 infant security, 519  
 as security risk, 57
- Lockers  
 access control, 122  
 as psychological deterrents, 31  
 security policies, 388–389
- Locks and keys  
 administration, 431–432  
 computer-based key accountability, 433–434  
 inspection, 123–124  
 interchangeable core, 432  
 inventorying, 436  
 key making, 435  
 lock changes, 434  
 lock installation, 434  
 master key systems, 432–433  
 padlocks, 435  
 push-button locks, 434  
 as safeguard, 124  
 types, 430–436
- Loma Linda Medical Center, 281
- Long Beach Memorial Medical Center (CA), 491, 621
- Long-term care facilities  
 deceased patients, 125  
 electronic access control, 458  
 employee property loss, 70  
*vs.* hospitals, 2  
 intercom systems, 458  
 mass notifications, 474  
 nursing shortage, 5–6  
 patient tagging, 349–350  
 security services, 129f  
 as speciality, 4  
 TJC standards, 8, 8t  
 as traditional environment, 19  
 workplace violence, 485, 491–492, 500
- Los Angeles riots, 56
- Lost and found, 124–125
- Loudspeaker notifications, 478f
- Louis Hospital (St. Croix), 61
- Lounge areas  
 access control, 519  
 fire risk, 59  
 infant security, 519  
 missing patients, 322  
 push-button locks, 434
- LPN, *see* Licensed practical nurse (LPN)
- LSMS, *see* Local Security Management Specialist (LSMS)

## M

- MacAlister, Don, 44–45
- Madrid Train Station Bombings, 66
- Magnetometer, 446–447
- Magstripe cards, 433–434, 455t
- Main, Brian, 461–462
- Main entrance  
 access control, 637  
 parking structures, 581  
 security response, 523–524
- Maintenance workers  
 investigations, 32  
 and keys, 435  
 in patient areas, 320  
 security history, 22–23
- Managed access control, 458
- Managed care programs  
 enrollment growth, 6  
 nonhospital healthcare, 4–5  
 physician impact, 6–7
- Management, *see* Security management
- Management selection, 163–164
- Management services  
 hospital security as, 23  
 security program responsibility, 33–34
- Manmade emergency events  
 active shooters, 613–614  
 bombs and threats, 601–605  
 civil disturbances, 611–613  
 fire prevention and control, 597–601  
 fire safety programming, 597

- gang/mob activities, 610–611
  - pandemic events, 613
  - strikes and picketing, 605–608
  - terrorism, 608–610
  - WMDs, 609
  - Marked vehicles
    - caregiver escort, 567–568
    - emergency planning, 618
    - personal transporter, 281
    - security carts, 280
    - sharing issues, 279
    - use of force options, 635t
  - Marking property
    - definition, 551
    - employee security training, 394
    - equipment tracking, 551
    - key making, 435
    - linens, 554
    - materials management, 549
    - purpose, 438
    - as safeguard, 28t
  - Massachusetts Departments of Public Health, 333
  - Massachusetts General Hospital (MA)
    - drug testing, 58–59
    - MPBS advice, 351
    - services, 110f
  - Massachusetts Nursing Association (MNA), 484, 485–486, 500
  - Massachusetts Society for Medical Research (MSMR), 555
  - Mass notifications
    - capability, 474–475
    - purpose, 641
    - systems, 478f
  - Master key systems, 432–433
  - Master name index, 312
  - Master security schedule
    - definition, 269
    - determination, 265
    - flexing, 266
    - staffing models, 629–630
  - Materials management
    - definition, 549–551
    - equipment, 551
    - goods and equipment distribution, 551
    - laundry access control, 554
    - laundry and linen control, 552
    - linen loss, 552
    - linen loss control, 553
    - linen loss figures, 552–554
    - linen marking, 554
    - off-campus security/safety, 575
    - property disposal, 551–552
    - purchasing and receiving, 549–550
    - scrubs losses, 553–554
    - storage, 550
  - Mayo Clinic, 218
  - MBPS, *see* Munchausen by Proxy Syndrome (MBPS)
  - McFarland, Derrick, 60
  - McGruff the Crime Dog*, 393
  - Mead Johnson Nutrition, 63, 515
  - Media relations
    - infant security, 524–525
    - security event attention, 622
  - Medical center security
    - definition, 547
    - double coverage shifts, 274
    - as healthcare system component, 1
    - investigation cooperation, 388
    - newsletters, 397–398
    - off-duty employees, 385
    - operational *vs.* nonoperational periods, 275–276
    - package inspection, 386
    - parking areas, 577
    - property identification, 388
    - public agency liaisons, 122
    - robbery issues, 65
    - security awareness, 92–94
    - staffing plans, 275t
    - staff lockers, 388–389
    - staff solicitation, 389
    - stalking incidents, 66
    - suspected property, 388
  - Medical clinic security
    - combative patients, 338–339, 341
    - information loss, 64
    - preventative patrol, 112
    - safeguards, 108
    - security education, 118
    - security responsibility, 108
    - theft, 109
  - Medical error *vs.* sentinel event, 12
  - Medical gasses
    - internal protection planning, 612
    - nitrous oxide, 560
    - oxygen, 560
    - security concerns, 559–560
  - Medical records, *see also* Health information management (HIM)
    - AMA form, 324
    - employee health record, 367
    - identity theft, 61
    - infant identification, 513
    - information disclosures, 547–548
    - information loss, 64
    - information release, 368, 369
    - information requests, 366–367
    - misuse, 71
    - officer training guidelines, 248t
    - parental security form, 516, 517f
    - Patient Bill of Rights, 319t
    - patient medical record, 367
    - personnel record, 368
    - privileged communication, 368
    - warrants/subpoenas, 368, 370
  - Medical records areas
    - access control, 121
    - alarm protection, 450–451, 452, 638
    - bomb search, 603–604
    - security sensitive areas, 505
    - video image as, 468
  - Medicare, *see also* Centers for Medicare and Medicaid Services (CMS)
    - anti-dumping law, 202
    - critical access hospitals, 4
  - Melendez v. City of Los Angeles*, 207–208
  - Memorial Hospital of Union County (OH), 55
  - Mental health facilities
    - closing issues, 7
    - security sensitive areas, 505, 506
    - security watch, 331
    - wandering patients, 348
  - Mental Health Intervention Team (Australia), 341–342
  - Merchant guard licenses, 202
  - Mercy University Hospital (Ireland), 225
  - Metal band seal, 436
  - Metal screening
    - emergency departments, 479–480
    - purpose, 641
    - security design, 446–447
  - Michelman, Bonnie, 165, 351
  - Micro digital video recorders, 467
  - Military officer recruitment, 182
  - Military style uniforms, 201–202, 202–203
  - Millwee, Steve, 490
  - Mini-mesh chain link fencing, 426
  - Minor crimes
    - concern for, 409
    - and law enforcement, 104
    - neighborhood profile, 208
    - priority, 20–21
  - Miranda rights, 178
  - Misconduct situations
    - disciplinary action, 196
    - FCRA, 408
    - investigation, 409–410
    - off-duty police, 142
    - performance management, 148
    - security function, 132
    - staff selection, 376
  - Missing patients
    - example policy, 323f
    - reporting, 69
    - search form example, 325f
    - security involvement, 322–325
  - Missing property
    - basic security services, 396t
    - deceased patients, 125
    - incident report, 303f, 305f, 402
    - investigation services, 396t
    - reporting, 402
    - security coordination, 102
    - security performance, 96t, 314f
    - supplemental reports, 307
  - Mission statement
    - management selection, 163
    - SMP, 86–87, 87f
  - MNA, *see* Massachusetts Nursing Association (MNA)
  - Mob issues, 592t, 610–611
  - Modified fixed post assignment, 272
  - Molotov cocktail, 436
  - Monetary awards, officer recruitment, 182
  - Mongeau, Dave, 467
  - Monitoring software, dispensing machines, 543–544
  - Monitoring station
    - communication device alerts, 584
    - patrol verification, 290
    - surface parking lots, 579–580
    - video surveillance, 460
  - Morale issues
    - and alarm systems, 450
    - attitude, 171
    - and performance, 171, 190
    - and protective vests, 225
    - and safety perception, 188–189
    - supervision, 165
    - and training programs, 233
    - undercover investigations, 419–420
    - and uniforms, 205–206
  - Moral responsibility, as security rationale, 21
  - Morva, William, 60
  - Motivation factors
    - leadership development, 256
    - psychological deterrents, 28–30
    - as supervisor responsibility, 172–173
  - MRI imaging, forensic patients, 346
  - MSMR, *see* Massachusetts Society for Medical Research (MSMR)
  - Multifacility security management control, 135–136, 137f
  - Multipurpose safes, 439
  - Munchausen by Proxy Syndrome (MBPS), 350–351, 489–490
  - Mutual aid planning, 617–618
- ## N
- NADDI, *see* National Association of Drug Diversion Investigators (NADDI)
  - Nahirny, Cathy, 36, 473, 508, 645
  - Name plates, uniform styles, 202
  - NAPBS, *see* National Association of Professional Background Screeners (NAPBS)
  - Narcotics
    - addiction problems, 59
    - badge access control, 514

- Narcotics (*continued*)
- Canada, 44
  - drug diversion, 542
  - electronic access control, 455
  - IAHSS training guidelines, 248t
  - operating room burglary, 55
  - police reporting, 104
  - robbery risk, 65
  - security risk assessment, 75
  - video surveillance, 462
- Narrative reports, 299–300
- Nashville General Hospital (TN), 520–521
- Nassau County Police (NCP), SPIN program, 362
- National Association of Drug Diversion Investigators (NADDI), 542–543
- National Association of Professional Background Screeners (NAPBS), 380
- National Center for Missing and Exploited Children (NCMEC)
- abduction risks, 63
  - abductor profile, 511
  - critical incident response plan, 522
  - family abductions, 527
  - infant abductions, 508
  - infant security guidelines, 521–522
  - infant tagging, 473, 645
  - parental education, 515–516
  - prevention education, 514
  - security program factors, 36–38
- National Crime Prevention Council (NCPC), 393
- National Fire Protection Association (NFPA), 41–42
- National Health Service (NHS)
- security administrator, 88–89
  - UK security program factors, 43
  - video surveillance, 461–462
  - violence costs, 225
  - violence perpetrator prosecution, 500
  - workplace violence, 483, 485
  - zero tolerance initiative, 497
- National Incident Management System (NIMS), 596, 597
- National Labor Relations Act, 63–64
- National Quality Forum (NQF), 42
- National Rifle Association (NRA), 215
- National standard of care, definition, 48
- Natural access control, CPTED, 441
- Natural disasters
- examples, 614
  - executive security primer, 621
  - as security risk, 51
- Natural surveillance, CPTED, 441–442
- NCMEC, *see* National Center for Missing and Exploited Children (NCMEC)
- NCP, *see* Nassau County Police (NCP)
- NCPC, *see* National Crime Prevention Council (NCPC)
- NCR, *see* No-carbon-required (NCR) paper reports
- Negative behavior
- attitude, 171
  - documentation, 175
  - vs.* false sense of security, 31
  - and natural access control, 441
  - preventative patrol, 112
  - security patrols, 30–31
- Negativity, performance monitoring, 171
- Neighborhood environment and arming officers, 208
- security strategic plan, 102–103
- Neighborhood watch, as community outreach, 103
- Neonatal intensive care units
- infant abductions, 510–511
  - risk assessment, 80f, 644
- Networking
- and employee morale, 171
  - with external agencies, 122
  - with peers, 160–161, 162
- Networks, computer
- information loss, 64
  - IP camera, 463, 464
  - IT, 557–558
  - mass notifications, 478f
  - technology implementation, 480
  - video analytics, 467
  - video surveillance, 469
- Network video recorders (NVRs), 458–459, 463
- New employee orientation
- presentation and handouts, 394–396
  - security programs, 646
  - security safeguards, 30
- Newman, Oscar, 441
- Newsletters
- employee education, 397–398
  - officer recruitment, 182
  - topics, 398t
- Newspaper recruitment ads, 182
- New York City Police Department (NYPD), 361
- NFPA, *see* National Fire Protection Association (NFPA)
- NHS, *see* National Health Service (NHS)
- Night entrances
- access control, 277, 534f
  - after hours access, 355
  - late night-shift employees, 586
- Night lighting
- area vulnerability, 429
  - flag etiquette, 128
  - off-campus facilities, 572–573
  - oxygen tank storage, 560
  - parking areas, 27
  - risk assessment, 75, 81
  - security data analysis, 153–154
  - security standards, 430f
- Nightstick
- equipment carried, 224–225
  - use of force options, 636
  - as weapon, 220
- NIMS, *see* National Incident Management System (NIMS)
- 9/11 terrorist attacks
- emergency planning impact, 592, 608–609
  - safety concerns after, 1
  - security effect, 622
  - security-police liaison, 360
  - U.S. hospital security history, 24
- Ninewells Hospital (UK), 461–462
- No-carbon-required (NCR) paper reports, 300
- Nonclinical facilities
- cash handling, 575
  - off-campus, 570, 576
  - security program structure, 573, 574f
  - security service impact, 129f
  - use of force, 243, 636, 632
- Nonfamily infant abductions
- from HCFs, 508
  - NCMEC trends, 36
  - as security risk, 63
- Nonfatal assaults
- patients, 487–488
  - workplace violence, 485, 642
- Nonhospital services, as healthcare component, 4–5
- Nonincident-driven investigations
- audits, 415
  - background checks, 414–415
  - spot checks/surveillance, 415–416
  - types, 414–416
- Nonoperational periods
- deployment plans, 275–276
  - patient care units, 276
- Nonscheduled duties
- definition, 151
  - security staffing, 149
- Nonverbal communication
- body language, 498–499
  - officer response, 292
  - officer training, 536
  - via report appearance, 299
- Northwestern Memorial Hospital (IL), 291–292
- Notebook and pen, equipment carried, 215
- Not-for-profit hospitals, definition, 3
- Nursery
- access control, 519
  - infant abductions, 509t, 510–511, 527, 644
  - parental security briefing form, 517f
  - standard of care, 48
  - video surveillance, 520t
- Nurses, *see also* Registered nurses (RNs)
- assaults, 54
  - emergency conditions, 614–615
  - infant security, 522
  - inpatient care, 320
  - interaction protocol, 536–537
  - narcotics addiction, 59
  - patient protection, 320
  - pharmacy access, 540
  - security incident reporting, 402
  - as security risks, 566
  - security watch, 329–330, 633
  - staffing issues, 5
  - triage, 339
  - unions, 44–45
  - violence threats, 622, 642
  - workplace violence, 483, 487–488
- Nursing homes
- assaults, 52–54
  - CMS regulations, 15
  - fire prevention, 597
  - homicide incidents, 60
  - lock systems, 291
  - as nonhospital healthcare, 4
  - officer's keys, 291
  - property loss, 69, 391–392
  - safeguards, 108
  - security responsibility, 108
  - security shifts, 274
  - staffing, 5
  - wandering patients, 348
  - workplace violence, 499–500
- NVRs, *see* Network video recorders (NVRs)
- Nylon duty belt, 225
- ## O
- Obedience
- canine patrols, 286
  - supervision styles, 164
- Objectiveness, investigators, 416–417
- Observation posts, parking areas, 579–580, 582
- Observation rooms
- ED security, 533–534
  - video surveillance, 470
- Observe and report
- inpatient assistance, 321
  - restraint training, 244
- Obstetrical unit control, 354
- Occupational Safety and Health Administration (OSHA)
- new officer training, 246
  - PPE standards, 218
  - security program factors, 38
  - workplace violence, 485, 486
- OCR, *see* Office of Civil Rights (OCR)
- OC spray, *see* Oleoresin capsicum (OC spray)
- Off-campus facilities

- access control, 570–571
  - alarms, 571
  - necessity, 563–576
  - night lighting, 572–573
  - nonclinical, 576
  - officer coverage, 571
  - patient treatment, 569
  - primary security safeguards, 570
  - security administrative structure, 573
  - security organization, 573–576, 574f
  - security responsibility, 570
  - security risk assessments, 564
  - security/safety representatives, 574–575
  - security signage, 572
  - SIR, 575
  - vehicle security patrols, 571–572
  - video surveillance, 571
  - Off-campus services
    - caregiver at risk, 566–567
    - home healthcare, 564–568
    - IAHSS guidelines, 565
    - patient at risk, 566
    - security practices/guidelines, 567–568
  - Off-duty employees
    - emergency staffing, 616–617
    - security issues, 385
  - Off-duty law enforcement
    - arming liabilities, 207
    - ED security staffing, 535–536
    - in emergency department, 339
    - as security staff, 142–143
    - U.S. hospital security history, 23
  - Offense report, *see* Security incident report (SIR)
  - Office of Civil Rights (OCR), 14
  - Office of the Porter, 22
  - Office of Privacy Commissioner for Personal Data (PCPD), 558–559
  - Officer presence, as use of force, 635f
  - OJT, *see* On-the-job training (OJT)
  - Oleoresin capsicum (OC spray), 221
  - One-way pager
    - equipment carried, 216
    - vs.* radio communication, 640
  - Ontario Nurses Association (Canada), 500
  - On-the-job training (OJT), 234, 235, 236f
  - Open house recruitment, 182
  - Operating rooms
    - as burglary target, 55
    - drug theft, 544
    - video surveillance, 469
  - Operational investigations, 409–410
  - “Operation Red Dragon,” 595
  - The Order of the Hospital, 22
  - Orderly environment maintenance, 111–112
  - Ordinances
    - licensing laws, 179
    - oxygen storage tanks, 560
    - parking control, 578
    - security program factors, 35f, 42–43
    - vehicle operation, 284
  - Organization chart
    - functional, 133–134
    - off-campus security, 573, 574f
    - security department, 133f, 134f, 136f
    - security program authority, 87, 89
    - security program example, 89f
  - Organization philosophy & culture and deployment patterns, 270
  - security department organization, 135–136
  - and security programs, 33
  - security staffing, 147, 153
  - uniform style, 199–200
  - Organization surveys, for TJC accreditation, 9–10
  - Ortiz, Richard, 284–286
  - OSHA, *see* Occupational Safety and Health Administration (OSHA)
  - Outdoor equipment storage, 426
  - Outpatient services
    - bed space, 4
    - definition, 3
    - as medical center component, 547
    - parking control, 577, 578
    - patient property handling, 353
    - as security risk, 57–58, 76f
  - Outside investigators
    - FCRA, 408
    - legal counsel, 407
    - for security investigations, 409–410
  - Outsourced services, *see also* Contract security staff
    - FTEs, 157
    - liability insurance, 557
    - management selection, 163
    - overview, 139–142
    - patient assistance, 321
    - vs.* proprietary, 139
    - security design, 8–9
    - security history, 23–24
    - security staff, 136, 139–142
    - staffing models, 138t
    - virtual patrol, 572
    - work shift, 269–270
  - Overflow areas, infant security, 527
  - Overhead announcements
    - active shooter events, 614
    - mass notifications, 474
    - for security communications, 116
  - Overt security activity, 394
  - Oxygen storage, 426, 560
- P**
- Package inspection
    - concentrated, 388
    - policy, 386–388
    - as support service, 127–128
  - Padlocks, 435
  - Pagers
    - mass notifications, 475, 641
    - necessary equipment, 216, 640
    - for security communications, 116
  - Palm readers, automated dispensing machines, 543–544
  - Pandemic event
    - emergency planning, 613
    - emergency preparedness, 592t
    - flu, 253–254
  - Panic button, *see also* Duress alarms
    - gift shops, 559
    - as holdup alarm, 452–453
    - off-campus facilities, 571
  - Parental security education, 517f, 518f, 515–518, 644
  - Parking areas
    - afternoon-shift employees, 586
    - automated controls, 587
    - as burglary target, 56
    - dangers, 577
    - demand for, 577
    - design priorities, 577–578
    - ED security, 531
    - electronic access control, 457–458
    - employee security knowledge, 403
    - external patrol, 277–278
    - fencing, 426
    - late-night shift employees, 586
    - natural surveillance, 441–442
    - night lighting, 572
    - parker types, 585–586
    - pay-for-parking, 587–588
    - personal communication devices, 584
    - risk assessment example, 77
    - rule enforcement, 117
  - safety reminder, 118f
  - security layering, 424
  - as security risk, 57
  - and security staffing, 155
  - signage, 582–584
  - space allocation, 587
  - street parking, 579
  - structures, 580–584
  - surface lots, 579–580
  - technological control, 589
  - traffic flow, 587
  - types, 579–584
  - valet service, 585
  - violators, 588–589
  - Parking shuttle service, 584–585
  - Parking structures
    - example, 581f
    - security concerns, 580–584
    - video surveillance, 582–584
  - Parking violation notice
    - and employee attitude, 404–405
    - purpose, 311
  - Partner practices, managed care impact, 6–7
  - Part-time security officers, *see also* Proprietary security staff
    - availability, 157
    - contract services, 140
    - cost containment, 449
    - costs, 139
    - vs.* full-time, 187–189
    - organization chart, 133f
    - senior market, 182
    - shift staffing, 152–153
    - weekend/holidays, 276
  - “Party line,” definition, 311
  - Par value, definition, 552
  - Pass-on record, 311–312
  - Passport scanners, 471
  - Patient Bill of Rights, 319, 319t
  - Patient care involvement
    - assistance, 320, 321–334
    - autistic patients, 342–344
    - behavioral health patients, 341–342
    - Bill of Rights, 319, 319t
    - combative patient, 338–341
    - ED security interactions, 536–537
    - ED security staffing, 535
    - emergency department, 339–340
    - forensic patients, 344–348, 349f
    - in general nursing unit, 341
    - IAHSS guidelines, 317
    - IAHSS patient search guidelines, 333
    - ICUs, 340–341
    - infant/pediatric patients, 350–351
    - infectious patient, 336–338
    - inpatients, 320, 321–334
    - large acreage facilities, 319
    - medical/dental clinics, 341
    - missing patients, 322–325
    - patient property, 351–353
    - patient restraint form, 332f
    - patient search, 331–334, 335f
    - property handling, 352–353
    - security role, 241–243, 632–634, 631
    - security watch, 329–334
    - VIP patient, 334–336, 337f
    - visiting hours, 354–355
    - visitors, 353–357
    - wandering patients, 348–350
  - Patient care units
    - active shooter events, 614
    - IAHSS security guidelines, 248t
    - missing patients, 324
    - patrol necessity, 276–277
    - risk assessment, 80f
    - video surveillance, 469–470
    - visiting hours, 355

- Patient elopement
  - IAHSS guidelines, 328
  - mental health patients, 342
  - prevention and response, 325–327
    - as security risk, 64–65
    - as TJC sentinel event, 12
- Patient losses, patient property, 69–70
- Patient medical records
  - HIM, 548
  - release, 370
  - release guidelines, 367, 369
- Patient monitoring
  - via electronic device, 327
  - recording rules, 468
  - video image quality, 639
- Patient property
  - checking in, 352
  - deceased patients, 39t, 125
    - handling, 352–353
    - and home caregivers, 566
  - investigations, 413–414
  - losses, 69–70
  - minor crimes, 409
  - policies and procedures, 93f
  - security performance standards, 314f
  - security policy, 93f
  - security problems, 351–353
  - security role, 351–353
- Patient risk group types
  - autistic patients, 342–344
  - behavioral health patients, 341–342
  - combative patient, 338–341
  - forensic patients, 344–348, 349f
  - infant/pediatric patients, 350–351
  - infectious patient, 336–338
  - VIP patient, 334–336
  - wandering patients, 348–350
- Patients
  - accident reporting, 26
  - accident risk, 71
  - assaults to, 52
  - deceased, 125–126
  - detention, 365–366
  - disaster risks, 72
  - ED security, 527–528
  - fire safety, 597, 599–600
  - forensic, 254
  - gifts from, 389
  - as healthcare stakeholders, 5
  - health information management, 547–556
  - home health security, 566
  - incorrect discharge, 71
  - off-campus treatment, 569
  - officer interaction, 179
  - police interaction, 364–371
  - relations with, 130
  - security awareness, 119
  - as security risk, 57–58
  - valuables, 126
  - violence, 484
  - vs.* visitor group, 317
  - workplace violence, 487–489
- Patient Safety and Quality Improvement Act of 2005, 42
- Patient volume
  - and security design, 446–447
  - security staffing, 149, 154, 630t
  - workplace violence, 642
- Patrols, *see also* Deployment plan
  - basic concepts, 277–292
  - basic duties, 272–276
  - battery-jumping service, 282–284
  - bicycle patrol, 280–281
  - canine, 284–286
  - as community outreach, 103
  - entrances/exits, 277
  - external, 277–278
  - external vehicles, 278–282
  - field supervisor, 135
  - first round, 288
  - frequency, 148, 151
  - internal, 286–287
  - new officer training, 245–246
  - off-campus facilities, 571–572
  - officer response, 292–293
  - overlapping areas, 273f
  - patient care units, 276–277
  - personal transporters, 281–282
  - problems, 293–294
  - as psychological deterrents, 30–31
  - reporting for duty, 288–289
  - role, 112
  - security carts, 280
  - security layering, 424
  - shift rotation, 289–290
  - surface parking lots, 579–580
  - techniques, 272, 632
  - transporting people, 283
  - vehicle damage, 284
  - vehicle equipment, 283–284
  - vehicle inspection report, 285f
  - vehicle operation, 284
  - vehicle patrols, 278–279
  - verification, 290–291
- Pay-for-parking programs, 587–588
- Payment handling
  - employee informants, 420–421
  - off-campus security, 575–576
- PBX operators
  - emergency call boxes, 474
  - incident reporting, 402
  - security communications, 116
  - security department organization, 136f
- Pediatric abductions
  - drills and exercises, 525
  - employee response, 396
  - IAHSS guidelines, 512
  - new employee training, 242f
  - prevention, 644
  - prevention/response, 647t
  - risks, 350–351
  - security risks/vulnerabilities, 627
  - statistics, 510
  - as TJC sentinel event, 97
  - vulnerable areas, 527
- Pediatric facilities
  - infant abductions, 510–511, 527
  - security concerns, 644–645
  - security risks, 350–351
  - security sensitive areas, 506
  - staffing, 5
  - visiting hours, 354
  - visitor control, 354
- Pedziwiatr, Kathleen, 320
- Peer networking
  - professional organizations, 162
  - security administrators, 160–161
- Pencil-sharpener camera, 467
- Pepper spray, 221
- Perceptions, *see* Safety perceptions; Security perceptions
- Performance standards
  - attendance, 169
  - attitude, 171–172
  - behavior documentation, 175
  - code of ethics, 191f
  - documentation, 173–176, 175–176, 174t
  - IAHSS guidelines, 96
  - improvement records, 313, 314f
  - monitoring, 169–172
  - officers, 190–196
  - performance management, 173–176
  - positive reinforcement, 192–193
  - problem employees, 176
  - rules and regulations, 193
  - sample log, 171t
  - security department, 96t
  - security programs, 647–648
  - security service survey, 405f
  - shift supervision, 167
  - SMP, 94–95
- Periodic Performance Review (PPR), 9–10, 37f
- Permit parking, 579
- Perpetrator, general
  - false sense of security, 31
  - incident report evidence, 524–525
  - infant abductions, 350
  - wrongdoing patterns, 414
- Perpetrator of workplace violence
  - categories, 487–491
  - profile, 501f
  - prosecution, 497, 500, 644
  - victim relationship, 487f
- Personal communication devices, 584
- Personal digital assistant (PDA), 228
- Personal entry, as infiltration method, 555
- Personal Health Information (PHI), 14
- Personal opinion, in reports, 306
- Personal property
  - audits, 123
  - minor crimes, 409
  - parking areas, 403
  - police role, 104
  - security role, 351
  - theft risk, 67
- Personal protective equipment (PPE), 218–219
- Personal safety
  - arming officers, 207
  - ED security, 538
  - employee classes, 397
- Personal space, and officer response, 292–293
- Personal transporter (PT) patrols, 281–282
- Personnel entrances, use policies, 30
- Personnel records, release, 368, 368–369, 370
- Pharmacies
  - access control, 120, 541
  - alarms, 450–451, 638
  - burglary, 55, 540
  - closed pharmacies, 541–542
  - drug diversion/theft, 542–544
  - duress alarms, 540–541
  - forged/altered prescriptions, 544
  - risk assessment, 267
  - robbery risks, 65
  - security issues, 539–544
  - security risk assessment, 75
  - security sensitive areas, 505, 506
  - video surveillance recording, 468
- PHI, *see* Personal Health Information (PHI)
- Phone trees, mass notifications, 478f
- Photographs
  - infant identification, 513
  - strike records, 607–608
- Physical abuse
  - child development center, 556–557
  - home caregivers, 566
  - home patient security, 566
  - long-term care, 485
  - pediatric patients, 350
  - staff selection process, 377
- Physical assault
  - as patient protection event, 43
  - threat assessment, 81f
  - types, 486
  - workplace violence, 485–486, 497
- Physical qualifications
  - new officer training, 243
  - officer selection, 183, 187
  - as staff assignment factor, 269
- Physical security safeguards
  - barriers, 424–428
  - basics, 423
  - bollards, 428

- bullet resistive glass, 437
- chain link fencing, 426
- command signs, 440
- computer-based key accountability, 430–431
- CPTED, 441–442
- decorative metal fencing, 426–427 and deployment patterns, 270
- ED security, 535
- examples, 27, 28f
- fastening down equipment, 437–438
- fencing, 424–427
- fire safe, 439
- glass protection, 436–437
- infant abductions, 519–520
- infant security, 644
- informational signs, 440
- interchangeable core locks, 432
- IT security, 558
- key inventories, 436
- lighting, 428–429
- lock changes, 434
- lock installation, 434
- locks and keys, 430–436
- lock system administration, 431–432
- master key systems, 432–433
- multipurpose safes, 439
- pharmacies, 540
- property marking, 438
- push-button locks, 434
- safes, 438–439
- seals, 436–437
- security design, 446, 636 and security risk assessment, 81f
- security staffing, 91, 153
- security strategic plan, 104–105
- signage, 439–441, 440–441
- system of perimeter design, 424
- trees/shrubs, 429–430
- Physician offices
  - after hours visitors, 355
  - as burglary target, 56
  - hostage taking, 59–60
  - security design, 106
  - security role, 4
  - staff property loss, 391–392
  - video surveillance, 460
  - window protection, 437
  - workplace violence, 491–492, 492
- Physicians
  - and alarm use, 450
  - ED protection, 622
  - emergency preparedness drills, 594–595
  - ID badges, 384
  - impersonation, 43, 62
  - managed care impact, 6–7
  - missing patient notification, 324
  - OSHA, 38
  - patient incidents, 536–537
  - patient search, 331–333
  - police liaison, 364
  - privileged communication, 368
  - security education, 118–119, 393, 497
  - security relations, 130
  - as security stakeholder, 5
  - security watch, 329–330
  - visiting schedule regulation, 567
  - workplace violence, 484, 488, 642–643
- Picketing
  - definition, 605–608
  - emergency preparedness, 592f
  - purpose, 606–607
  - strikes, 607–608
  - supply lines, 608
- Planetree, Inc., 33, 121
- “Planting” objects, investigations, 414
- Plastic seals, 436
- Platte Valley Medical Center (CO), 346
- Police departments, *see also* Law enforcement agencies
  - emergency planning, 618–619
  - liaison programs, 361–362
  - security call policies, 363–364
  - vs.* security investigation, 408–409
- Police holds, 366
- Police officers
  - emergency room activity, 365
  - off-duty, *see* Off-duty law enforcement
  - patient detention, 365–366
  - patient/employee interactions, 364–371
  - potential conflict, 372
  - security history, 23
  - security staffing, 148
- Police response time, environmental profile, 208
- Police room, ED training, 539
- Policies and procedures
  - business office/cashiers, 557
  - child development centers, 556–557
  - contraband, 390–391
  - drug testing, 391
  - ED security, 530, 537
  - examples, 93f
  - investigation cooperation, 388
  - operational, 296–298
  - outside investigators, 409–410
  - package inspection, 386–388
  - patient elopement, 327
  - patient search, 335f
  - police calls, 363–364
  - problem areas, 297–298
  - procedure definition, 297
  - property disposal, 551–552
  - records retention, 314–315
  - security audit, 415
  - security department, 92
  - security-oriented employment guidelines, 384–392
  - security programs, 34–35
  - security-related, 646–647, 647f
  - security strategic plan, 101–102
  - signage control, 440–441
  - surplus/damaged property, 390
  - systems security programs, 146
  - VIP patients, 337f
  - workplace violence, 494–495
- Politician patients, 334
- Polo style uniforms, 203, 204f
- Polygraph tests, 186
- Pooling Resources in Defense of Our Environment (PRIDE), 361–362
- Pop-up message mass notifications, 478f
- Positive reinforcement, 192–193
- Post assignments
  - fixed-post, *see* Fixed-post assignments
  - staff scheduling factors, 269
  - and training time, 152
  - types, 271–272
- Posters
  - employee education, 398
  - fire safety training, 600–601
  - mass notifications, 478f
- Post orders, definition, 296–297
- Postpartum units
  - infant abductions, 510–511, 516
  - as security sensitive area, 522
- Power loss, as security concern, 120
- POWER principle, 537, 538t
- PPE, *see* Personal protective equipment (PPE)
- PR, *see* Privacy Rule (PR)
- Preadmission registration, patient property, 351
- Prejudices, investigator attributes, 416–417
- Preliminary investigation
  - follow-up relationship, 413
  - incident investigation phases, 411–412
- Prescriptions
  - forged, 144
  - forged/altered, 544
- Preservice training, security staffing, 152
- PRIDE, *see* Pooling Resources in Defense of Our Environment (PRIDE)
- Pride, as officer selection criteria, 183
- Prisoners, police interactions, 366
- Privacy Act of 1974, 547–548
- Privacy laws, and Virginia Tech massacre, 14–15
- Privacy officer
  - information requests, 366–367
  - responsibilities, 548
  - video recordings, 468
- Privacy Rule (PR), HIPAA overview, 14
- Privileged communication, 368, 370
- Probation status, disciplinary action, 196
- Problem employees, handling, 176
- Problem solving abilities, 184f
- Procedure, *see* Policies and procedures
- Product distribution policies, 389
- Professional Certification Board of ASIS International, 73
- Professionalism
  - performance monitoring, 172
  - security principles, 194f
- Professional memberships, 162
- Profession *vs.* professional, 45
- Promotion, *see* Job promotion
- Property damage
  - civil disturbances, 611
  - from disturbances, 57
  - emergencies, 120
  - fire/explosion, 59
  - investigation, 409–410
  - labor disputes, 64
  - pandemic events, 613
  - patient security assistance, 321
  - security program effectiveness, 98
  - security program objectives, 32, 624
  - security sensitive areas, 505
  - during strikes, 606
  - terrorism, 66
  - as threat, 51
  - video surveillance, 639
  - workplace violence, 492–494, 643
- Property lines
  - and area crime data, 151
  - fencing, 424–426, 426, 611–612
  - grounds lighting, 428–429
  - missing patients, 323
  - system of perimeters, 424, 425f
- Property losses
  - employee property, 70–71
  - fires, 72
  - healthcare facilities, 69
  - internal patrol, 287
  - investigations, 32
  - law enforcement involvement, 362–363
  - minor crimes, 409
  - off-duty employees, 385
  - patients, 69–70
  - prevention, 48, 391–392
  - reporting, 69
  - robbery, 65
  - security coordination, 102
  - small facilities, 156
  - staff property, 391–392
  - surveillance, 416
- Property pass system
  - example, 387f
  - package inspection, 386
- Property protection
  - basic records, 301
  - disposal, 549, 551–552
  - employee background checks, 555
  - via firearms, 206



- Property protection (*continued*)  
 home patient security, 566  
 inspection policy, 388  
 medical centers, 388  
 as moral responsibility, 21  
 off-site facilities, 570  
 parking areas, 578, 588, 579  
 security function, 131  
 security sensitive areas, 505  
 surplus/damaged, 390  
 UK programs, 43  
 via weapons, 220
- Proprietary alarm systems, 453
- Proprietary security staff, *see also* In-house security staff  
 advantages/disadvantages, 138–139  
 contract combination, 142  
*vs.* contract costs, 140  
 and leadership, 626  
 licensing, 178–179  
 management selection, 163  
 from outsourced, 139–140  
 staffing models, 138f, 138t  
 as staff type, 136  
 training, 152, 233  
 U.S. security history, 23–24
- Protective vests, 224–225
- Protocol, *see also* Policies and procedures  
 definition, 297  
 ED security, 536–537  
 forensic patients, 349f  
 outside investigators, 409–410  
 patient elopement, 326–327
- Provena Saint Joseph Hospital (IL), 336
- Providence Everett Medical Center (WA), 463–464
- Provona Morey Medical Center (IL), 59–60
- Proximity cards  
 for access control, 455t  
 computer-based key accountability, 433–434  
 visitor management systems, 471
- Psychological patients, security role, 348–350
- Psychological security safeguards  
 examples, 27, 28t  
 false sense of security, 31–32  
 motivation factors, 28–30  
 overview, 27–32  
 security design, 446  
 security patrols, 30–31  
 security safeguards, 30  
 signage, 423
- Psychological tests, officer selection, 186
- PT, *see* Personal transporter (PT) patrols
- Public-employee relations, 22
- Public entrances  
 access control, 570  
 security master plan, 445
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002, 219
- Public relations, 130
- Public safety liaison  
 adverse police relations, 372  
 basic considerations, 94  
 and central security station, 447  
 community programs, 371  
 coordination with, 103  
 dynamics, 359–361  
 emergency room activity, 365  
 employee health records release, 367, 370  
 grand jury subpoenas, 368  
 information release guidelines, 367–368  
 information requests, 366–367  
 law enforcement contact, 371–372  
 law enforcement service requests, 362–364  
 nonpolice liaison, 372–373  
 off-campus facilities, 564  
 overview, 359  
 patient detention, 365–366  
 patient/employee interactions, 364–371  
 patient medical records release, 367, 369, 370  
 personnel records release, 368, 368–369, 370  
 police call policies, 363–364  
 police and security cooperative programs, 361–362  
 privileged communications, 368  
 response times, 152  
 search warrants, 368  
 security department, 371–372
- Public safety response time, staffing considerations, 152
- Punitive damage awards, 21
- Purchased services approach, 143–144
- Purchasing and receiving security, 549–550
- Push-button locks, 434
- Pyxis machines, 58
- ## Q
- Quasicalentralization security philosophy, 135, 135
- Quiet rooms, 533–534, 534f
- ## R
- Rabun, John, 36, 508
- RACE, 600
- Radio equipment  
 central security station, 448  
 equipment carried, 216  
 mass notifications, 478f  
 purpose, 640  
 for security communications, 116
- Radio frequency identification technology (RFID), 475, 641
- Radio frequency (RF) devices  
 alarms, 452  
 automated parking control, 587  
 ID badges, 383  
 infant tagging, 473  
 parking area security, 584  
 patient elopement, 327  
 wandering patients, 349–350
- Radiological dispersal device (RDD), 609
- Radiological weapons, 609–610
- Radio repeater system, 449–450
- Ram-raiding, 428
- Random rotation, 272
- Rape  
 emergency rooms, 365  
 risk assessment, 80f  
 as security risk, 52–54  
 and staff selection, 377  
 as TJC sentinel event, 12, 13f  
 workplace violence, 484t
- RATER model, 245
- Razor-ribbon fencing, 426
- RDD, *see* Radiological dispersal device (RDD)
- Receptionist  
 access control, 519, 570  
 car theft case, 109  
 ED security, 532  
 workplace violence, 489
- Recognition of performance, 168, 172–173, 190, 192–193, 192–193
- Recognition pins, 202
- Recognition software, 354–355, 463
- Records  
 administrative needs, 298–300  
 basic types, 301–306  
 documentation policy, 298–299  
 employee health, 367
- infant monitoring, 521  
 keeping current, 313  
 as memory system, 295–296  
 patient, 367  
 performance improvement, 313, 314f  
 problem areas, 297–298  
 retention policy, 314–315  
 SIR, 302–306  
 SMP, 94  
 strikes, 607–608  
 training, 262, 262f
- Record safe, 439
- Recruitment options, 180–182
- Red Bank Veterinary Hospital, 19
- Red-lined positions, 189
- Redundant monitoring  
 central security station, 519  
 electronic system integration, 444  
 strategic cameras, 468–469
- Referral recruitment programs, 180, 181f
- Registered nurses (RNs)  
 education and training, 232  
 imposter risk, 62  
 as security risk, 144  
 staffing issues, 5
- Relative safety, definition, 19–20
- Reliability, RATER model, 245
- Reporting levels  
 security function, 131–136  
 security history, 23  
 SMP, 89, 626
- Reporting for patrol duty, 288–289
- Reporting systems  
 employee informants, 420–421  
 as inspection supplement, 26  
 legislation, 42  
 patrol verification, 290  
 property losses, 69  
 security incident reports, 302  
 security programs, 146
- Reports, *see also* Incident reports  
 annual security management plan, 313  
 computer-generated, 300–301  
 daily activity, 309–311  
 distribution, 128  
 formats, 299–300, 300  
 for information exchange, 296  
 master name index, 312  
 monthly/periodic, 312–313  
 parking violation notice, 311  
 pass-on record, 311–312  
 program effectiveness evaluation, 313  
 security condition, 307–315  
 SMP, 94  
 supplemental, 307  
 training, 262, 262f  
 writing training, 244–245, 632
- Requests for service response, 113–116
- Researchers relations, 130
- Research laboratories  
 protection, 554–556  
 security sensitive areas, 505, 506
- Response times  
 and building design, 154  
 central security station, 447  
 daily activity report, 311  
 deployment objectives, 268  
 patient elopement, 325–327  
 police, 208, 372  
 public safety response time, 152  
 security performance, 314f  
 service calls, 148, 150f, 151, 630t  
 shared central station, 449–450  
 staffing considerations, 150f, 150–151
- Responsiveness  
 officers, 292–293  
 RATER model, 245  
 as success factor, 268

- Restraining orders
  - HIPAA rules, 14
  - imposters, 62
  - stalking, 66
  - workplace violence, 496, 501–502
- Restraint basics
  - CMS guidelines, 7, 15, 38, 220, 224
  - combative patient, 338–339
  - deaths, 12
  - ED security, 528
  - forensic patients, 254, 344–345, 645
  - handcuffs, 217, 217–218, 346, 636
  - Patient Bill of Rights, 319t
  - policies, 636
  - sample form, 331, 332f
  - security performance, 187t
  - security program objectives, 624
  - security watch, 331
  - threat policy, 495
  - use of force options, 635t
  - workplace violence, 488–489, 642–643
- Restraint training
  - IAHSS curriculum, 248t
  - new officers, 244
  - officers, 536
  - security role, 632
  - staff competency, 632
- Restricted access capabilities, considerations, 456–457
- Resuscitation equipment, patrol vehicles, 284
- Retinal scanners, 543–544
- Retirement organizations, for officer recruitment, 182
- Return on Investment (ROI)
  - new officer training, 235
  - security administrator traits, 625
  - security programs, 34
  - security risk assessment, 77
  - security training, 630–631
  - service response times, 151
  - from training, 234–235
- Reviewable event, TJC sentinel events, 12
- RF, *see* Radio frequency (RF) devices
- RFID, *see* Radio frequency identification technology (RFID)
- Risk assessment, *see also* Security risks/vulnerabilities
  - basic sources, 76f
  - as continuous process, 82
  - degree of threat, 75–77
  - executive primer, 626
  - guidelines, 75
  - home caregiver, 566–567
  - home patients, 566
  - home practices/guidelines, 567–568
  - IAHSS guidelines, 82–83
  - identification, 627–628
  - via incident reports, 267
  - methodologies, 74–75
  - off-campus facilities, 564
  - and physical safeguards, 81f
  - qualified persons, 73–74
  - risk identification, 72–82
  - and safeguards, 77–81
  - SMP 89–90
  - and staffing, 155
  - workplace violence, 486
  - worksheet example, 77, 80f
- Risk management
  - assisting patients, 321
  - components, 26, 27f
  - concept, 23–24
  - definition, 26
  - department-specific security training, 396
  - experience, 73
  - HIPAA, 14
  - hospital leadership, 594, 595t
  - HVA, 51
  - investigations, 407–408
  - manager role, 26
  - officer training, 252t
  - patient elopement, 327
  - patient search, 331–333
  - reporting levels, 132, 626
  - security coordination, 102
  - security master plan, 445, 627
  - security services, 129f
  - surveillance recording, 468
  - U.S. hospital security history, 23–24
- Rivas v. Nationwide Personal Security Corp.*, 177
- RNs, *see* Registered nurses (RNs)
- Robbery
  - business office/cashiers, 557
  - cashiers, 557
  - deployment plan, 267
  - parking control, 577
  - pay-for-parking areas, 588
  - pharmacies, 540
  - security incident report, 305f
  - security newsletter topics, 398t
  - security policies, 647t
  - as security risk, 53f, 65, 80f, 81f
  - security sensitive areas, 505
  - security training, 397
  - workplace violence, 486, 489, 643
- ROI, *see* Return on Investment (ROI)
- Role play training, 261
- Roof security, 561–562
- Rope, patrol equipment, 284
- Rules and regulations
  - disciplinary action, 195
  - employment application forms, 378
  - employment conditions, 30
  - employment guidelines, 384
  - enforcement, 120, 375
  - forensic patients, 254
  - investigations, 407
  - officer performance, 193
  - on-the-job training, 236f
  - parking control, 117
  - performance expectations, 191
  - performance management, 173
  - personnel conduct, 193
  - shift supervision, 167
  - vehicle operation, 284
  - workplace violence, 497
- S**
- Sabotage risk, 56
- Safeguards
  - active shooters, 613–614
  - business offices, 557
  - cashiers, 557
  - child development centers, 556–557
  - ED security, 530, 535
  - electronic, *see* Electronic security safeguards
  - individual decision making, 30
  - infant security, 519–520
  - lock and key basics, 124
  - off-campus patient care, 570
  - parking structures, 580–582
  - patient information, 547
  - pharmacy burglary, 540
  - physical, *see* Physical security safeguards
  - psychological, *see* Psychological security safeguards
  - security design, 636
  - and security risk assessment, 77–81
  - security risks/vulnerabilities, 628
  - smaller organizations, 108
  - types, 27
  - VIP patient, 334–336
  - wandering patients, 348–349
- Safeguard Their Tomorrows*, 515
- Safe rooms, ED security, 534–535
- Safes
  - alarm protection, 450–451
  - as physical security, 438–439
- Safety affidavit, firearms training, 214f
- Safety-Net facilities, definition, 3
- Safety perceptions, *see also* Security perceptions
  - customer service, 111, 626
  - e-mail broadcasts, 401
  - and employee attitudes, 404–405
  - intercoms, 457–458
  - leadership development, 255–256
  - parking areas, 579
  - part-time officers, 188–189
  - personal safety, 121
  - security force, 179, 629
  - security staffing, 150f
  - security stakeholders, 153–154
  - via signage, 441
  - vehicle patrols, 282
- Safety precautions, ED staff education, 538
- Safety-related risks
  - accidents, 66–67
  - fires, 597
- Safety Services components, 25–26
- San Francisco General Hospital (CA), 55
- Sarratt, Walt, 530–531
- Scaglione, Ben, 464
- Scheduled routine functions
  - definition, 151
  - staffing considerations, 148, 150f, 630t
- Scheduled special functions, 148, 630t
- Schedule II narcotics, 67
- Schoolfield, Dale, 336
- Scrubs, loss, 553–554
- Seals, as physical security, 436
- Search warrants, 368, 370
- Secret Service liaison, 122
- Sector patrol, 272
- Security administrators
  - activities, 160–161
  - body of knowledge, 162
  - department-specific training, 396
  - emergency event staffing, 616–617
  - ethical standards, 163–164
  - external protection planning, 611–612
  - female officers, 184
  - first patrol information, 288
  - healthcare executive primer, 625–626
  - hospital watch, 405–406
  - membership participation, 162
  - mutual aid planning, 617–618
  - necessity, 7
  - pass-on records, 312
  - patient property, 352
  - seminars and education, 162
  - service opportunities, 109
  - SMP guidelines, 88
  - support cycle, 132
  - video surveillance recording, 468
- Security advisor, definition, 22
- Security awareness
  - components, 397–401
  - as education element, 119
  - handbill example, 401f
  - handouts, 398, 399f, 400f
  - importance, 403–404
  - via meetings, 401
  - newsletters, 397–398, 398t
  - SMP, 92–94
  - websites/e-mail broadcasts, 398–401
- Security basics
  - access control, 637–638
  - administrators, 625–626
  - alarm systems, 638

- Security basics (*continued*)
- care provider issues, 622
  - challenges, 623
  - community standards, 628–629
  - customer service, 626
  - design, 636–637
  - employee role, 645–646
  - event examples, 621
  - forensic patients, 645
  - infant/pediatric security, 644–645
  - master plan, 626
  - media attention, 622
  - objectives, 623–624
  - patient involvement, 632–634
  - performance, 647–648
  - policies and procedures, 646–647, 647t
  - reporting structure, 626
  - risks/vulnerabilities, 626
  - staff competency, 631–632
  - staffing, 629–630, 630t
  - technology, 639–641, 641–642
  - training expectations, 630–631
  - uniforms, 634
  - use of force, 634–636
  - video surveillance, 638–639
  - workplace violence, 642–645
- Security carts, advantages, 280
- Security communications
- active shooter event, 614
  - basic function, 109–111
  - central security station, 447
  - compartmentalization, 533
  - critical incident response plan, 522
  - emergency call boxes, 474
  - emergency reaction, 120
  - hazards, 246
  - ICS, 596
  - infant security, 524–525
  - with military, 595
  - monitoring center, 135
  - off-campus facilities, 564
  - officer response, 292
  - overview, 116
  - post assignments, 271
  - by radio, 640
  - security master plan, 445
  - security and safety representative, 574–575
  - shared central station, 449–450
  - shift supervision, 167
  - strikes, 605
  - supervision, 168
  - system inspection, 123–124
- Security condition report
- example, 309f
  - purpose, 307–315
- Security cooperative programs
- examples, 361–362
  - FBI counterintelligence domain project, 362
  - SPIN, 362
- Security department
- authorized staffing level, 90t
  - creation, 23
  - emergency event staffing, 616–617
  - healthcare systems, 135–136, 136f
  - incident response plan, 507–508
  - key inventorying, 436
  - law enforcement liaison, 359–361, 371–372, 372t
  - nonpolice liaison, 372–373
  - orderly environment, 111–112
  - organization chart, 133f, 134f, 133–134
  - organization overview, 131
  - parking complaints, 578
  - performance standards, 96t
  - policy and procedure, 92
  - public safety liaison, 359
  - reporting levels, 131–136
- U.S. hospital security history, 23–24
- Security design
- access control, 454, 541, 637
  - basic considerations, 446–447, 637
  - ED considerations, 531–535
  - elopement prevention, 327
  - external organizations impact, 44–45
  - parking structures, 580–582
  - system of perimeters, 424
- Security dispatcher
- shared central security station, 449–450
  - uniforms, 203–204
- Security escorts
- home caregivers, 567–568
  - providing, 403
  - street parking, 579
- Security fair, for crime prevention, 401
- Security force administration
- CHPA, 161
  - code of ethics, 191f
  - communication, 168
  - components, 159
  - confidentiality agreement, 195f
  - CPP exam, 162
  - disciplinary action, 195–196
  - full- *vs.* part-time officers, 187–189
  - fundamental principles, 194f
  - management, 159–164
  - management selection, 163–164
  - motivation, 172–173
  - officer authority, 176–177
  - officer licensing, 178–179
  - officer relationships, 172
  - officers, 176–179
  - officer selection criteria, 182–185
  - officer selection process, 185–187
  - officer traits, 184f
  - performance documentation, 173–176
  - performance expectations, 190–196
  - performance management, 173–176
  - performance monitoring, 169–172
  - positive reinforcement, 192–193
  - rules and regulations, 193
  - security personnel selection, 179–187
  - shift supervision, 167
  - special police commission, 177–178
  - supervision, 164–172
  - supervisor selection, 165–167
  - training, 168–169
- Security history, 22–25
- Security incident report (SIR)
- as assessment lesson, 628
  - as basic record type, 302–306
  - classifications, 114f
  - ease of, 112–113
  - example, 303f
  - filing considerations, 304–306
  - IAHSS guidelines, 302
  - master name index, 312
  - off-campus facilities, 575
  - security watch, 330–331
  - SMP, 95f
  - staffing issues, 152
  - statistics, 304, 305f
  - supplemental reports, 307, 308f
- Security layering, definition, 424
- Security management
- access control, 120–122
  - applicant background investigation, 119
  - audits, 123–124
  - communications, 116
  - customer service, 111
  - education and training, 118–119
  - vs.* emergency management, 24
  - external agency liaisons, 122–123
  - incident reporting/investigation, 112–113
  - internal/external emergency reaction, 119–120
  - locks and keys, 124
  - parking and traffic control, 117
  - performance documentation, 173
  - preventative patrol, 112
  - requests for service response, 113–116
  - rules and regulations, 120
  - security force, 159, 159–164
  - support services, 124–129
- Security management planning
- components, 85
  - cycle, 100
  - reporting structure, 626
  - security strategic plan, 100–106
  - SMP, 85
- Security management plan (SMP)
- authorized staffing level, 90t
  - CCTV use, 91f
  - data collection, 112–113
  - definition, 85
  - duties and activities, 91
  - education, 92–94
  - IAHSS guidelines, 86
  - incident report, 95f
  - inclusiveness, 85
  - mission statement, 86–87, 87f
  - organization chart, 89f
  - performance standards, 94–95, 96t
  - physical safeguards, 91
  - policy and procedure, 92, 93f
  - program authority, 87
  - public safety agency liaison, 94
  - purpose, 313
  - records and reports, 94
  - risk assessment evaluation, 89–90
  - security administrator guidelines, 88
  - security sensitive areas, 90
  - staff position descriptions, 90
  - staff training, 92
  - TJC standards, 95–100
- Security Management Service (SMS)
- administrator guidelines, 88–89
  - UK security program factors, 43
  - workplace violence, 483
- Security master plan
- components, 445–446
  - necessity, 626–627
- Security mission statement
- example, 87f
  - management selection, 163
  - SMP, 86–87
- Security officers
- after-hours visitor control, 356
  - arming
    - community standard, 211–212
    - deterrent value, 208
    - disarming circumstances, 212
    - environmental profile, 208–211
    - factors, 206–213
    - firearms training, 214f
    - liability, 207–208
    - personal safety, 207
    - personnel quality, 212
    - policies, 213
    - trends, 213
    - vulnerability, 207
  - weapon/holster/ammunition, 212–213
  - weapons experience, 211
  - authority, 176–177
  - autistic patient response, 343t
  - CCTV setup, 461f
  - chronological history, 192f
  - code of ethics, 191f
  - via contract services, 140
  - customer-oriented services, 109
  - disciplinary action, 195–196
  - ED staffing, 536
  - equipment, *see* Equipment carried full- *vs.* part-time, 187–189

- on investigative loan, 419–420
- and job status, 109f
- licensing, 178–179
- locked area access, 121–122
- off-campus coverage, 571
- parking services, 117
- patient care involvement, 632–634
- patrol keys, 291–292
- performance expectations, 190–196
- picket lines, 606–607
- positive reinforcement, 192–193
- recruitment, 180–182
- response, 292–293
- responsibilities, 176–179
- retention, 190
- security watch, 330
- selection, 179–187
- selection criteria, 182–185
- selection process, 185–187
- special police commission, 177–178
- staff/line positions, 149–150
- supervisor relationships, 172
- Taser affidavit training, 222f
- training
  - adequate, 231
  - aggression management, 241–243, 243t
  - annual program topics, 252t
  - basic concepts, 233
  - bulletin example, 260f
  - competency verification, 240f, 240–241
  - considerations, 255
  - contemporary issues, 252–255, 633t
  - critical task focused, 235–241, 242f
  - customer service, 245
  - definition, 234
  - ED, 536
  - elective, 255
  - emergency preparedness, 254–255
  - equipment, 227
  - expectations, 630–631
  - forensic patient delivery, 254, 346–347
  - gang issues, 252–253
  - IAHSS Advanced Training, 249–250, 250t
  - IAHSS Basic Training, 247–249, 248t
  - IAHSS guidelines, 233–234
  - IAHSS Progressive Certification, 246–250
  - IAHSS Supervisory Training, 250–251, 251t
  - key topics, 241–246
  - new officers, 235–246
  - on-the-job, 235, 236f
  - OSHA compliance, 246
  - overview, 235–246
  - pandemic flu, 253–254
  - patient care, 241–243
  - patrol techniques, 245–246
  - records, 262f, 262
  - report writing, 244–245
  - resources, 258–262
  - restraint training, 244
  - specialized/supplemental, 251–255
  - steps, 231–232
  - Tasers, 222f
  - types, 234–235
  - use of force, 243–244
  - WMDs, 253–254, 253t
- traits, 184f
- turnover, 233
- uniform styles, 634
- use of force, 226, 226–227
- visitor contact, 353–357
- wage compensation, 189
- and workplace violence, 488–489
- Security operations manual, 227–228
- Security-oriented employment guidelines
  - contraband, 390–391
  - drug testing, 391
  - EAP, 391
  - employee security responsibility, 385
  - employee time-recording, 390
  - investigation cooperation, 388
  - off-duty employees, 385
  - overview, 384–392
  - package inspection, 386–388
  - patient/family gifts, 389
  - staff lockers, 388–389
  - staff property loss, 391–392
  - staff solicitation/product distribution, 389
  - surplus/damaged property, 390
  - weapons policy, 385–386
- Security perceptions, *see also* Safety perceptions
  - during audits, 124
  - batons, 224
  - community standards, 211–212, 628–629
  - forensic patients, 345–346
  - incident report filing, 32
  - metal screening, 479, 641
  - officers of people, 320
  - organization leadership, 33–34
  - security master plan, 446
  - security staffing, 150f
  - security technology, 642
  - system testing, 480
  - territorial reinforcement, 442
  - uniforms, 199–200, 201–202
  - vehicle patrols, 279
- Security Police Information Network (SPIN), 362
- Security precautions
  - as crime deterrent, 404
  - gangs, 252–253
  - HIM, 548–549
  - ICU, 340
  - infant/pediatric patients, 350
  - infant security, 521–522
  - parental education, 516–518
  - patient elopement, 326, 537
  - patient property, 70
  - requests for information, 366–367
  - storage areas, 550
  - supply lines, 608
  - threat response team, 496
  - VIP patients, 80f, 334
- Security presentations
  - employee education, 394, 646
  - new employee orientation, 30, 149–150, 394–396
  - security awareness, 118–119
  - self-directed, 397
  - staff education, 397
  - TJC standards, 98
  - video materials, 259
- Security principles list, 194f
- Security program basics
  - ASIS International, 41
  - authority positions, 87
  - basic objectives, 40, 623–624
  - body of knowledge, 45–48
  - CMS, 38
  - considerations, 19–21
  - corporate policy, 34–35
  - development, 27
  - education and training, 92–94, 118–119
  - effectiveness evaluation, 313
  - employee role, 645–646
  - evolution, 22–25
  - external forces, 35–45, 35t
  - focus, 107–108
  - functions, 107, 109–111
  - funding, 34
  - IAHSS, 38–42, 39t
  - internal forces, 33–35
  - and law enforcement, 20
  - vs.* law enforcement, 20t
  - leadership factors, 33–34
  - legislation factors, 42–43
  - NCMC factors, 36–38
  - NFPA, 41–42
  - objectives, 32–35
  - off-campus administration, 573
  - off-campus cash/payments, 575–576
  - off-campus organization, 574f, 573–576
  - off-campus representatives, 574–575
  - off-campus SIR, 575
  - ordinance factors, 42–43
  - organization chart, 89f
  - organization philosophy/culture, 33
  - performance benchmarking, 647–648
  - rationale, 21–22
  - as reflection of leader, 108
  - and risk assessment, 73
  - smaller organizations, 108
  - State Health Department factors, 42–43
  - structure, 107
  - TJC factors, 35–36
  - U.S. changes, 25t
- Security risks/vulnerabilities
  - arming officers, 207
  - assaults, 52–54
  - bomb threats, 54–55
  - burglary, 55–56
  - categories, 52
  - dissident group actions, 56–57
  - disturbances, 57–58
  - drug abuse, 58–59
  - embezzlement, 59
  - employee theft, 67–71
  - examples, 53f
  - fire/explosion, 59
  - homicide, 60–61
  - hostage taking, 59–60
  - identification, 51, 627–628
  - identity theft, 61
  - imposters, 62
  - information loss, 64
  - kickbacks/fraud, 62–63
  - kidnapping/abduction, 63
  - labor actions, 63–64
  - patient elopement, 64–65
  - primary, 52–72
  - related risk examples, 71
  - robbery, 65
  - stalking, 66
  - terrorism, 66
  - theft, 66–67
- Security room, 539
- Security Rule (SR), 14
- Security *vs.* safety, 25–26
- Security and Safety department
  - off-campus representatives, 574–575
  - U.S. history, 23
- Security scheduling, *see also* Work shifts
  - as administrative function, 268–270
  - analysis, 141
  - attendance, 169
  - daily activity report, 309
  - deployment example, 273
  - double coverage, 274
  - flexible, 390
  - full- *vs.* part-time officers, 187
  - home visits, 567
  - officer coverage, 571
  - officer selection criteria, 182–183
  - parking areas, 582
  - post assignments, 272
  - preventative patrol, 112
  - program organization chart, 89f
  - reporting for duty, 288
  - small facilities, 156
  - soft data analysis, 152–153
  - staffing problems, 157

- Security sensitive areas
  - access control, 456, 507
  - categories, 505–508
  - definition, 505
  - ED, *see* Emergency department (ED)
  - IAHSS guidelines, 506
  - pharmacies, 539–544
  - SMP identification, 90
  - staff education, 507
- Security services
  - basic listing, 396t
  - organization impact, 129f
  - performance survey, 405f
  - sample list, 110f
- Security staff
  - basic models, 138f
  - commissioned police officers, 143
  - competency, 631–632
  - considerations, 150f
  - corporate approach, 144–147
  - during emergencies, 616–617
  - emergency department, 535–537, 537–539
  - function-based uniforms, 200
  - IAHSS guidelines, 147–149
  - infant abduction response, 523–524
  - IT security, 558
  - model comparison, 138t
  - off-duty law enforcement, 142–143
  - outsourcing, 139–142
  - proprietary and contract, 142
  - proprietary staff, 138–139
  - recruitment monetary award, 182
  - scheduling factors, 268–270
  - shared services approach, 143–144
  - size, 147
  - small facilities, 155–157
  - SMP position descriptions, 90
  - staffing levels, 150–155
  - staff/line positions, 149–150
  - subjective considerations, 154–155
  - training, 92
  - types, 136–147
  - use of force options, 634–636
- Security staffing plan
  - executive primer, 629–630
  - flexing, 266–267
  - objective criteria, 630t
- Security strategic plan
  - building design, 106
  - components, 100–106, 101f
  - crime prevention, 102–103
  - criminal justice interface, 104
  - definition, 85
  - employee/staff role, 105
  - organization-specific, 106, 627
  - organization-wide coordination, 101–102
  - physical security safeguards, 104–105
  - public safety coordination, 103
- Security supplemental report
  - example, 308f
  - purpose, 307
- Security Technician, definition, 149–150
- Security technology, *see also* Electronic security systems
  - access control, 120
  - effectiveness, 641–642
  - for parking control, 589
  - training resources, 259
  - types, 639–641
  - U.S. hospital security history, 24
  - visiting hours control, 354–355
- Security watch
  - nurse responsibility, 633
  - as patient involvement, 329–334
  - patient search, 331–334
- Selective call feature, radios, 216
- Self-defense classes, 119, 397
- Self-directed security education, 397
- Senior market officer recruitment, 182
- Sensitivity training, 243
- Sentinel events, TJC
  - policies, 11–14
  - by year, 13f
- Serious assaults
  - critical incident response plan, 507–508
  - incident increase, 19, 622, 624
  - as security risk, 52
  - vulnerability, 207
- Service call response time
  - security staffing, 148, 151
  - staffing considerations, 150f, 151
  - staffing criteria, 630t
- Severe acute respiratory syndrome (SARS), 613
- Sexual abuse, home caregivers, 566
- Sexual assault
  - definition, 52
  - employee expectations, 270
  - employee security knowledge, 402
  - incident reporting, 402
  - investigation, 407–408
  - as patient protection event, 43
  - workplace violence, 484
- Sexual harassment, security investigations, 409–410
- Sexual molestation, child development centers, 556–557
- Shackles, forensic patients, 346
- Shared central security station, 449–450
- Shared services, as security staff, 143–144
- Sharp container theft risk, 67
- Shift rotation, importance, 289–290
- Shift supervision
  - communication, 168
  - tasks, 167
- Shipments, support services, 127
- Short-term acute care, definition, 3
- Shrubs, as physical security, 429–430
- Shuttle service, parking areas, 584–585
- SICDS, *see* Sudden In Custody Death Syndrome (SICDS)
- Signage
  - command signs, 440
  - control, 440–441
  - informational signs, 440
  - off-campus security, 572
  - parking areas, 582–584
  - as physical security, 423, 440
  - security layering, 424
  - types, 439–441
  - violence language, 501f
- Signing bonus, officer recruitment, 181
- Signs and notices, as psychological deterrents, 31
- Simple assault
  - definition, 52
  - workplace violence, 491f
- Simplify Your Workday* (Hemphill), 295
- Sinai Hospital (MD), 281
- SIR, *see* Security incident report (SIR)
- Sir Charles Gardiner Hospital (Australia), 500
- Sirens, mass notifications, 478f
- Sit-down consoles, 449t
- Situational event, workplace violence, 491–492
- Situation step, security strategic plan, 101
- Size of grounds, staffing issues, 154
- Skilled care, definition, 3
- Skill level factors
  - listening skills, 498
  - officer selection criteria, 179, 183, 185
  - security principles, 194f
  - staff scheduling, 269
  - supervisory training, 251t
- Slote, Leslie M., 176
- Smith, Tom, 160–161
- Smithfield Hospital, 22
- Smoke detector camera, 467
- SMP, *see* Security management plan (SMP)
- SMS, *see* Security Management Service (SMS); Text messaging (SMS) notifications
- Snowstorm emergency planning, 614, 592t
- S.O.A.R., *see* Special Operations and Response (S.O.A.R.)
- Sociability traits, officers, 184f
- Socializing, as patrol problem, 293
- Social Services Act, 22
- Societal conventions, as psychological deterrents, 28–29
- Soft-bodied armor vest, 224
- Soft data analysis, security staffing, 152–154
- Software
  - automatic drug dispensing, 543–544
  - electronic access control systems, 455
  - facial recognition, 354–355
  - IP cameras, 464
  - parking control, 589
  - for staff scheduling, 269
- Sold services, as security staff, 143–144
- Solicitation policy, 389
- South Jersey Healthcare Regional Medical Center, 514–515
- Space allocation, parking areas, 587
- Spartanburg Regional Healthcare System (SC), 463
- Special assignments, security staffing, 149
- Special care nursery, infant abductions, 527
- Specialized sitter uniforms, 203
- Special Operations and Response (S.O.A.R.), 595
- Special police commission officers, 177–178
- Specialty clinics, as security sensitive area, 506
- SPIN, *see* Security Police Information Network (SPIN)
- “Spoliation,” 314–315
- Spontaneous event, workplace violence, 492
- Spot-checking
  - as audit, 123
  - as nonincident investigation, 415–416
- Spotlight, patrol vehicle equipment, 283
- Sprint/Nextel Direct Connect, 216
- SR, *see* Security Rule (SR)
- St. Anthony’s Central Hospital (CO), 537
- St. John’s Hospital (MO), 220–221
- St. Louis Children’s Hospital (MO), 251–252
- Staff, general, *see also* Security staff
  - abduction prevention education, 514–515
  - accident reporting, 26
  - active shooter events, 614
  - assaults to, 52, 54
  - child development centers, 556–557
  - customer service, 111
  - department-specific security training, 396
  - fire safety, 599–600
  - as healthcare stakeholders, 5
  - infant security, 513–514, 516, 523, 515t
  - medical care facilities, 5–6
  - positions, 149–150
  - protection program role, 105
  - security sensitive areas, 507
  - vs.* security staff levels, 154
  - selection via due diligence, 376–377
  - solicitation, 389
- Staff entrance control, 587
- Staff response time, staffing considerations, 150–151
- Stairwell security
  - access control, 519
  - assaults, 54

- badges, 355
  - CCTV, 91f, 473
  - civil disturbances, 611
  - door locking, 366
  - lighting inspections, 123–124
  - locking, 48
  - parking garage intercoms, 457–458
  - parking structures, 581, 581f
  - patrolling, 287
  - risk assessment, 76f
  - video surveillance, 582–583
  - workplace violence, 492
  - Stakeholders
    - healthcare environment, 5
    - safety perception, 153–154
  - Stalking risks, 66
  - Standard of care, definition, 48
  - Standards, definition, 47
  - State Health Department, 42–43
  - State of security, via military and law enforcement, 20
  - Stewart, Rhonda, 489
  - Stewart, Robert, 60
  - Stolen property
    - disciplinary actions, 195
    - in employee lockers, 31
    - family *vs.* caregiver, 567
    - hiding in landscaping, 429–430
    - lost and found, 124–125
    - during picketing, 605
    - transport suspicions, 387
  - Stone wall perimeter, 424
  - Storage issues
    - bomb threat prevention, 602
    - nitrous oxide tanks, 560
    - oxygen tanks, 560
  - Storerooms
    - access control, 121
    - alarm protection, 450–451
    - infant security, 519
    - materials management, 550
    - officer's keys, 291
  - Street parking, 579
  - Strike action committee, 605
  - Strike control team, 605
  - Strikes
    - definition, 605–608
    - emergency preparedness, 592t
    - initial stages, 606
    - nonstriking employees, 606
    - record keeping, 607–608
    - supply lines, 608
  - Students
    - college recruitment, 182
    - emergency events, 614–615
    - ID badges, 384, 514
    - pharmacies, 539
    - security relations, 130
    - security training, 232
  - Substance abuse
    - employee remedies, 20–21
    - workplace violence, 487–488, 490t
  - Sudbury Regional Hospital (Canada), 55
  - Sudden In Custody Death Syndrome (SICDS), 217–218
  - Suicide, as TJC sentinel event, 12
  - Sunnybrook Health Sciences Center (Canada), 349–350
  - Supervision
    - communication, 168
    - inspection reports, 170f
    - leadership principles, 164–172
    - performance log, 171t
    - performance monitoring, 169–172
    - shift supervision, 167, 168
    - supervisor selection, 165–167
    - systems security program, 144–145
    - training, 168–169
  - Supervisors
    - officer relationships, 172
    - performance documentation, 173, 175–176
    - performance management, 173
    - uniform insignia, 202
  - Supervisory Training Manual for Healthcare Security Personnel*, 250
  - Suppliers-security contact, 353
  - Supply system
    - laundry/linen, 552
    - linen loss, 552–553
    - during strikes, 608
  - Support services
    - cash registers, 126–127
    - deceased patients, 125–126
    - emergency messages, 126
    - emergency shipments, 127
    - flag etiquette, 128
    - lost and found, 124–125
    - miscellaneous examples, 128–129
    - overview, 124–129
    - package check, 127–128
    - patient valuables, 126
    - report/equipment distribution, 128
    - resource conservation, 125
    - support cycle, 132
  - Surface parking lots, 579–580
  - Surge, 616
  - Surge groups, pandemic events, 613
  - Surgery rooms
    - access control, 120, 454, 637
    - video surveillance, 469
  - Surgical patient unit control, 354
  - Surplus property policy, 390
  - Surreptitious entry, as infiltration, 555
  - Surveillance
    - after-hours visitors, 356
    - animal activist infiltrations, 555
    - central security station, 448
    - CPTED, 441–442
    - internal protection planning, 612
    - as nonincident investigation, 415–416
    - security layering, 424
    - as security role, 112
    - video, *see* Video surveillance
  - Survey basics
    - CMS, 15
    - employee attitudes, 404–405
    - employee safety perception, 404–405
    - for entrance/exit security, 277
    - for environmental profiles, 208
    - external audits as, 123
    - vs.* risk assessment, 73
    - as risk assessment information, 76f
    - security initiatives, 399
    - services performance, 405f
    - for TJC accreditation, 9–10
    - wage surveys, 189
  - Surveyors, *see* The Joint Commission (TJC) surveyors
  - Suspects
    - FCRA, 408
    - firearms policy, 213
    - incident response, 523
    - interrogation, 411–412, 417–418
    - law enforcement liaison, 104
    - master name index, 312
    - patterns, 414
    - use of force, 635t
  - Suspension, as disciplinary action, 196
  - Suspicious behavior
    - reporting, 524–525
    - spotting, 523
  - Swine flu virus, 613
  - System of perimeters
    - alarms, 450–451
    - design, 424
    - security as, 75, 425f
  - Systems integration, electronic security, 444
  - Systems security program
    - management control, 135–136
    - security staffing, 144–147
- ## T
- Table tents, employee education, 398
  - Tafoya, William, 372
  - Tailgating, video verification, 460
  - Tangibility, RATER model, 245
  - Targeted victim
    - restraining orders, 501–502
    - workplace violence, 491
  - Targeted violence
    - IAHSS guidelines, 501–502
    - mass notifications, 474, 641
    - temporary security conditions, 155
    - VIP patients, 80f
  - Target step, security strategic plan, 101
  - Tasers
    - affidavit training, 222f
    - equipment carried, 219–221
    - as use of force, 636
  - Task Force Report on Private Security, 359–360
  - Taylor, Latrice, 489–490
  - TCH, *see* The Children's Hospital (TCH)
  - Technical knowledge, management selection, 163
  - Technology, *see* Electronic security systems; Information technology (IT); Security technology
  - Technology closets/rooms, access control, 120
  - Telephone hotlines
    - bomb threats, 602–603
    - employee informants, 420–421
  - Telephone stickers, as psychological deterrents, 31, 31f
  - Television announcements, mass notifications, 478f
  - Temporary incapacitation, as use of force, 635t
  - Territorial reinforcement, CPTED, 442
  - Terrorism, *see also* 9/11 terrorist attacks
    - biological/radiological weapons, 609–610
    - ecoterrorism, 554–555
    - emergency planning, 608–610
    - emergency preparedness, 592t
    - security effectiveness, 443
    - as security risk, 66
    - WMDs, 609
  - Text messaging (SMS) notifications, 478f
  - The Children's Hospital (TCH), 563–564
  - The Children's Hospital (TCH) Network of Care, 563–564
  - Theft overview, 66–67, *see also* Auto thefts; Drug theft; Employee theft; Identity theft; Robbery
  - The Joint Commission (TJC)
    - birthing unit security, 350
    - CMS overview, 15
    - education and training, 118–119
    - emergency planning, 592–594
    - emergency preparedness drills, 594–595
    - employee security training, 394, 646
    - Environment of Care time line, 37f
    - EOC committee, 10–11
    - fire risks, 72
    - forensic patients, 344–345, 346
    - healthcare executive primer, 621
    - ID badges, 381–382, 382–383
    - imposter incident, 62
    - organization surveys, 9–10
    - OSHA relationship, 38
    - parking and traffic control, 117
    - patient elopement policy, 326

- The Joint Commission (TJC) (*continued*)  
 patient rights, 319  
 prisoner handling, 366  
 required reading, 160  
 response time tests, 268  
 security administration, 7  
 security data collection, 112–113  
 security program effectiveness evaluation, 313  
 security program factors, 42  
 security program performance, 647  
 security report position, 626  
 security sensitive areas, 505  
 security services performance, 405  
 security standards, 35–36  
 seminars, 162  
 sentinel events, 13f, 11–14  
 SMP standards, 95–100  
 standards design and implementation, 8–9  
 standards manual, 8t  
 standards and mission, 7–14  
 standards scoring, 9–10  
 surveyor identification, 472, 472t  
 systems security management control, 135  
 U.S. hospital security history, 24  
 workplace violence, 488–489, 642–643
- The Joint Commission (TJC) surveyors  
 badge program problems, 382–383  
 competency-based training, 239–240  
 employee preparation for, 398  
 and EOC, 11  
 identification issues, 472, 472t  
 imposters, 62  
 and security education, 118–119  
 security knowledge, 36
- Thermal imaging cameras, 467
- Thoroughness, officer traits, 184f
- Threat assessment  
 management training, 494  
 officer selection process, 185  
 and security response, 81f  
 security service impact, 129f  
 threat identification, 628  
 workplace violence, 642
- Threatening behavior, investigation, 409–410
- The Threat from Within: Workplace Violence* (Millwee), 490
- Threat policy, workplace violence, 494–495, 643
- Threat response, workplace violence, 495–496
- Threat response team, workplace violence, 495–496
- Tiller, George, 563
- Time recording, employees, 390
- TJC, *see* The Joint Commission (TJC)
- Tool set, patrol vehicle equipment, 284
- Tornado emergency planning 614, 592t
- Tow cable, patrol vehicle equipment, 284
- Towing, parking violators, 588
- Town hall meetings, security awareness, 401
- Tracer methodology, 9, 37f
- Traditional style uniforms, 201–202
- Traffic control  
 as basic service, 117  
 and building design, 106  
 cones, 284  
 internal protection planning, 612  
 parking area flow, 587
- Training, *see* Education and training; Security officers, training
- Transmitters  
 alarm systems, 451  
 asset tracking, 475, 641  
 for surveillance investigations, 416
- Transportation accidents, 615, 616–617, 592t
- Transportation Service Authority, terrorism preparedness, 608–609
- Transportation services  
 assisted living, 2  
 external patrol, 282  
 off-campus facilities, 564, 573  
 parking shuttle, 585  
 as security function, 39t  
 security vehicle use, 283  
 U.S. hospital history, 23–24
- Trash collection system, patrolling, 287
- Travel planning, emergency, 618–619
- Trees  
 and exterior lighting, 429  
 as physical security, 429–430
- Triage, ED security, 532
- Tri-fold brochures, employee education, 398
- Triggers, violence prevention, 498
- Trustworthiness, security principles, 194f
- Tuberculosis, 246
- Turner, James T., 485
- Turnover rate  
 security staffing, 152  
 and training, 233
- Two-way radio  
 bomb search, 603–604  
 emergency call boxes, 474  
 equipment carried, 216, 640  
 incident reporting, 402  
 internal protection planning, 612  
 security practices, 567  
 shared central security station, 449–450
- U**
- UIR, *see* Unusual incident report (UIR)
- UL, *see* Underwriters Laboratory (UL)
- Unannounced inspections, 123
- Unconscious motivation, psychological deterrents, 29
- Undercover investigations  
 considerations, 418–420  
 employee informants, 420–421  
 employee participation, 394  
 IAHSS guidelines, 418–419  
 operatives, 123
- Underwriters Laboratory (UL)  
 central security station, 452  
 fire safe, 439  
 multipurpose safe, 439
- Unethical behavior, and leadership, 164
- Uniform Deduction authorization, 205f
- Uniforms  
 appropriate style, 634  
 blazer style, 202–203, 203f  
 emergency planning, 618  
 function-based style, 200, 201t  
 military style, 201–202  
 organizational philosophy, 199–200  
 patient disruption, 276–277  
 polo style, 203, 204f  
 staff scheduling factors, 270  
 style advantages/disadvantages, 200t  
 style determination, 199–204  
 supply/maintenance, 204–206  
 traditional style, 201f  
 variety, 199–206
- Unions  
 in-house staffing, 139  
 labor actions, 63–64  
 security impact, 44–45  
 strikes/picketing, 605  
 strike stages, 606
- Unit concept, fire containment, 598–599
- Unit dose systems, as security risk, 58
- United Kingdom  
 hospital security history, 22  
 protective vests, 225  
 security administrator guidelines, 88–89  
 security program factors, 43  
 video surveillance, 461–462  
 violence perpetrator prosecution, 500  
 workplace violence, 483
- United States Border Patrol agent uniforms, 202
- United States Constitution, officer knowledge, 178
- University of Michigan Medical Center (UMC), 56
- University of North Carolina Hospitals (NC), 143, 322
- University of Pittsburgh Medical Center, 65
- University of Wisconsin Hospitals, 470, 595
- Unrestricted patrol function, 272
- Unusual behavior, security training, 515t
- Unusual incident report (UIR)  
 inadequate investigations, 413–414  
*vs.* SIR, 302
- Unwanted behavior  
 deterrence, 403, 532  
 eye contact deterrence, 111  
 natural surveillance, 441–442
- Use of force  
 IAHSS guidelines, 226–227  
 new officer training, 243–244  
 officers, 226  
 options, 634–636, 635t  
 security role, 632
- Utilities failure emergency planning, 592t
- V**
- VA, *see* Veterans Administration (VA) Hospital
- Vagrants, 427
- Valet parking, 585
- Valuables  
 during disasters, 72  
 fire safes, 439  
 investigations, 413  
 minor crimes, 409  
 parking areas, 403, 584  
 policies, 126, 236f, 297, 647t  
 protection system, 70  
 security incidents, 113, 114f  
 security position functions, 76f  
 security watch, 331  
 storage in safes, 438, 439  
 TJC standards, 98
- Vandalism  
 extinguishers, 600  
 glass, 436  
 grounds lighting, 428–429  
 home caregiver security, 566  
 HVA, 51  
 incident reports, 305f, 402  
 investigation, 409–410  
 lighting, 428–429  
 parking areas, 578, 587  
 patrol deployments, 273  
 research labs, 554–555  
 security performance, 96t  
 security risk basics, 53f, 81f  
 security services, 396t
- VAPPSA, *see* Virginia Police and Private Security Alliance (VAPPSA)
- Vehicle patrols  
 advantages/disadvantages, 278–282, 279t  
 basic considerations, 278–279  
 bicycle patrol, 280–281

- damage, 284
  - equipment, 283–284
  - function, 278–279
  - inspection report, 285f
  - off-campus facilities, 571–572
  - operation, 284
  - personal transporters, 281–282
  - security carts, 280
  - transporting people, 283
  - Vehicle towing, parking violators, 588
  - Vendor issues
    - access control, 121, 447, 480, 640
    - accident reporting, 117–118
    - fraud, 63
    - investigative firms, 409–410
    - IT security, 558
    - kickbacks, 62
    - laundry, 552
    - linens, 554
    - parking control, 585–586, 578
    - purchasing/receiving, 550
    - relations with, 130
    - security contact, 353
    - security mission statement, 86–87
    - strikes, 606, 608
    - vetting, 380
    - visitor management, 471
  - Verbal abuse
    - care providers, 622
    - home caregivers, 566
    - home patient security, 566
    - visitors, 489
  - Verbal communication
    - officer response, 292
    - use of force, 635t
  - Verbal warning
    - as disciplinary action, 196
    - as use of force, 635t
  - Veterans Administration (VA) Hospital, 67
  - Veterans Administration (VA) National Center for Patient Safety, 325–326
  - Victim-perpetrator mix, 487f
  - Video analytics
    - benefits, 466–467
    - vs. RFID, 479
  - Video door phones, 457–458
  - Video monitoring
    - patient rooms, 470, 470, 639
    - and response capability, 584
  - Video surveillance, *see also* Closed circuit television (CCTV)
    - after-hours visitors, 356
    - analog vs. digital, 465f
    - basic use, 460–463
    - business office/cashiers, 557
    - central security station, 448
    - child development centers, 556–557
    - covert cameras, 467–468
    - CPTED, 441–442
    - dummy cameras, 470–471
    - ED security, 532
    - equipment, 463–468
    - gift shops, 559
    - infant security, 519–520, 520t, 644
    - IP cameras, 464–466
    - location and image quality, 638–639
    - monitoring, 468–469
    - as nonincident investigation, 415–416
    - off-campus facilities, 571
    - overview, 458–459
    - parking structures, 582–584
    - patient care areas, 469–470
    - recording, 468
    - security layering, 424
    - as security role, 112
    - surface parking lots, 579–580
    - thermal imaging cameras, 467
    - video analytics, 466–467
  - Video verification, definition, 460
  - Village Board, standard of care, 48
  - Violence
    - criminal definition, 484
    - domestic, *see* Domestic violence patient
    - employee, 484, 490–491
    - targeted, *see* Targeted violence
    - workplace, *see* Workplace violence
  - Violence in the Medical Care Setting: A Survival Guide* (Turner), 485
  - Violence Prevention in Health Care Facilities Act (NJ), 499–500
  - Violent behavior
    - de-escalation, 241–243
    - legislative action, 499
    - reporting, 494
    - security competence, 631
  - VIP patients, 334–336, 337f
  - Virginia Police and Private Security Alliance (VAPPSA), 361
  - Virginia Tech tragedy, 14–15, 474, 641
  - Visibility
    - deployment goals, 268
    - staff scheduling factors, 270
  - Visitor issues
    - accident reporting, 26, 117–118
    - accident risk, 71
    - after-hours, 355–356
    - assaults to, 52, 54
    - designated visiting hours, 354–355
    - disaster risks, 72
    - ED security, 527–528, 531–532, 537
    - emergency messages, 126
    - fire safety, 599–600
    - large acreage facilities, 319
    - medical/dental clinics, 341
    - officer interaction, 179
    - vs. patient group, 317
    - relations with, 130
    - robbery risks, 65
    - security awareness, 119
    - security contact, 353–357
    - workplace violence, 487–491, 489–490, 643
  - Visitor management systems
    - characteristics, 471–472
    - purpose, 640
  - Voice evacuation, 478f
  - Vulnerabilities, *see* Security risks/vulnerabilities
- ## W
- Wackenhut Training Institute (FL), 232
  - Wage compensation, security officers, 189
  - Wage surveys, 189
  - Waiting areas
    - access control, 570
    - after-hours visitors, 356
    - canine patrol, 284–286
    - ED security, 531–532
    - emergency department, 339, 440, 535–536
    - family consult room, 534
    - ICUs, 340
    - infant security, 510–511, 515t, 644
    - orderly environments, 111–112
    - parking shuttle service, 585
    - reception, 532
    - security design, 531
    - violence, 483–484
  - Wake Forest University Baptist Hospital (NC), 543–544
  - Walk-in areas
    - ED security, 531–532, 534f
    - reception desk, 532
  - Walton, Sam, 111
  - Wandering patients
    - vs. leaving AMA, 324
    - security involvement, 348–350
    - video surveillance, 462
  - Warren, Bryan, 278
  - Washington Hospital Center (DC), 610
  - Watch-clock, 290
  - Water loss, as security concern, 120
  - Water retention ponds, 426
  - Weapons
    - biological/radiological, 609–610
    - employee policy, 385–386
    - officer experience, 211
    - security effectiveness, 443
    - type, 212–213
    - WMDs, *see* Weapons of Mass Destruction (WMDs)
    - workplace violence, 488t
  - Weapons of Mass Destruction (WMDs)
    - emergency planning, 609
    - security training, 253–254, 253t
  - Weather conditions
    - emergency planning, 614–615
    - as security concern, 120
  - Weather radios, mass notifications, 478f
  - Web notifications, 478f
  - Websites, employee education, 398–401
  - Weekends deployment plans, 276
  - Well-baby units, 510–511, 644
  - West Virginia Hospital Association, 500
  - What Parents Need To Know*, 515–516
  - Wheaton Franciscan All Saints Healthcare (WI), 201–202
  - Wheelchairs
    - forensic patients, 345–346
    - marking, 438
    - providing, 128
  - Wide-area radio network, 216, 449–450
  - Wilson, O.W., 411–412
  - Wire seals, 436
  - WMDs, *see* Weapons of Mass Destruction (WMDs)
  - Work order, security report as, 309
  - Workplace violence
    - actual vs. threat, 485
    - categories, 484, 491–492
    - common weapons, 488t
    - definition, 483
    - emergency department, 483–484
    - employees, 490–491
    - forensic patients, 645
    - IAHSS guidelines, 493–494, 501–502
    - as industry problem, 483
    - infant/pediatric patients, 644–645
    - as international problem, 485
    - legislative action, 499–500
    - level of concern, 642–645
    - management, 492–494
    - patients, 487–489
    - perpetrator profile, 501f
    - perpetrator prosecution, 500
    - perpetrators/visitors, 487f, 487–491
    - preparation/response steps, 643
    - prevention, 496–502
    - prevention and management, 494
    - prevention training, 497–499
    - restraining orders, 501–502
    - risk factors, 486
    - risk identification, 627
    - safe rooms, 534–535
    - signage language, 501f



- specific acts, 491f
  - as threat, 483–484
  - threat policy, 494–495
  - threat response team, 495–496
  - time and location, 492
  - underreporting, 485–486
  - visitors, 489–490
  - Workplace Violence: Before, During, and After* (Heskett), 485
  - Work shifts, *see also* Security scheduling
    - double coverage, 274
    - in-house *vs.* outsourced staff, 269–270
    - and parking, 586, 586
    - pass-on record, 311
    - patrol assignments, 273
    - rotation importance, 289–290
    - staff scheduling factors, 268–269
  - World Health Organization, 613
  - Written warning disciplinary action, 196
  - Wrong doers
    - employee informants, 420–421
    - patterns, 414
    - psychological deterrence, 27, 32
- X**
- X-ray imaging
    - ED layout, 534f
    - forensic patients, 346
- Y**
- Yuma Regional Medical Center (AZ), 537
- Z**
- Zero tolerance policy
    - negative attitudes, 172
    - workplace violence, 497
  - Zone patrol, function, 272 *Partendes*  
*terum publium di, nericat usulat,*  
*pro nox ses*