

# Healthcare Security Supplement



# Assessing Security Staffing

## What You Need to Review When Evaluating Healthcare Security

**H**ealthcare environments are often open to the public, located in high traffic areas and accessed by many staff, patients and visitors daily. Additionally, this is a highly regulated industry that requires constant focus on compliance.

As a result, healthcare facilities are unique and challenging environments to secure. Patients, hospital staff and the public need to be protected from a wide variety of potential problems. The scenarios could range from a bioterrorism attack to robbery, or stolen identification to a violent altercation.

Healthcare facility directors often wonder if there are resources to help them determine the number of full-time security officers needed to staff their facility. Unfortunately, there is not a specific metric for how much personnel is needed. A customized approach is best in every instance as the security needs and goals of every healthcare facility differ.

When evaluating security, healthcare leaders should consider the following:

- What is the location of the facility – rural or urban?
- What are the size and demands of the hospital?
- What is the local crime rate?
- What is the hospital culture?
- What security technology is utilized and what is needed?
- What are your expectations of your security staff?
- Is your current program contributing to patient satisfaction?
- What training has been provided to security and hospital staff?

Partnering with knowledgeable security professionals to answer these questions and



Local Response | National Support

evaluate your situation will help you make the best security staffing decisions. In addition to quality security officers, you also need the right leader overseeing the program to ensure that your goals are being met. The right individual will have a vision for the future, as well as focus for today.

Maintaining a comprehensive security program involves a continuous evaluation process to determine the effectiveness and ultimately, its success. Much more than bed count or square footage needs to be considered when determining an adequate level of security personnel.

For more information on improving the effectiveness of your security program and to see your frequently asked questions answered by Ken Bukowski, AlliedBarton’s Vice President of Healthcare, visit: [AlliedBarton.com/HealthcareQandA](http://AlliedBarton.com/HealthcareQandA).

**For more information contact:**

Kenneth Bukowski

866.825.5433

[kenneth.bukowski@alliedbarton.com](mailto:kenneth.bukowski@alliedbarton.com)

# Management of Threats

by Lisa Pryse Terry, CHPA, CPP

Any situation is better managed before it gets out of hand. Management of threats in the sensitive healthcare environment is one of the top priorities in the field of healthcare security, and begins with identifying the threats in your facility. Emergency Department (ED) violence is of particular concern to hospital administrators, as the number of violent events has escalated in the past few years.

The best strategy to mitigate threats and risk of violence is a combination of predefined actions:

- Decreasing threats
- Blocking opportunities
- Minimizing costs to life or property

Threat management strategies involve a multi-pronged approach to security improvement. Workplace violence assessments, healthcare threat assessments, and engineering/technology controls should be integrated into the process. These approaches allow healthcare security professionals to evaluate, plan, mitigate, respond, and recover from threats

or actual events. Getting the C-suite buy-in is critical to a proactive threat management plan and effective strategy. It's important to demonstrate the overall benefits of various strategies to optimize the opportunity to decrease threats and enhance the patient experience. When you demonstrate the impact of inaction vs. proactive planning, you can build a strong case for proactive security strategies. Utilizing a proactive approach to ED security can save money and lives. The message of zero tolerance for violence trickles from the top down. To effectively manage and minimize threats, it's important to ensure ongoing commitment from the C-suite and executive leadership for security improvements and enhancements. Threat management is a process, not an event. It requires leaders to:

- Assess and prepare
- Evaluate and test
- Respond and recover
- Assess and refine

---

*continued on page 4*

C-suite commitment is central to the success of the hospital security plan and the ongoing process. On a blog post, Greg Goynes, vice president of marketing at IntelliCentrics, shared seven ways hospital and health system leaders can promote a culture of safety and continually support threat management processes:

- Publicly support patient safety efforts
- Empower staff members to take control of patient safety, and institute accountability
- Involve all relevant staffers or stakeholders in patient safety efforts
- Ensure staff members feel responsible for identifying potential safety issues
- Require all staff members, including C-suite leaders, to follow all safety rules and regulations
- Executives should ensure any employee with a safety concern has an accessible, non-punitive avenue for expressing that concern
- The C-suite must continue to make patient safety a priority and follow through on all initiatives. Once you have executive-level support, a well-planned, proactive security management strategy and process revolves around:
  - Reasonable level of security—Ensure the security of the overall environment and identify areas of probable conflict.
  - Organizational threat policy—The policy supports efforts to minimize threats, manage threats, and develop/implement policies and procedures.
  - Response plan—Managing threats includes responding to actual events. A response plan enables the organization to recognize, react, and respond to events and behaviors of concern.
  - Recovery—The final step in managing threats is to develop a solid recovery plan to ensure operations resume as quickly and efficiently as possible after an event occurs.

Once everyone is on board with the necessity of threat management strategies, it's time to

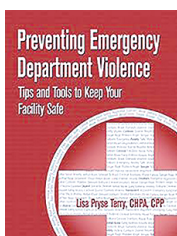
get down to the business of planning. The first step in solidifying an overall healthcare security plan is completion of a thorough healthcare threat assessment to assess your threat level, conducted by qualified healthcare security professionals. This assessment identifies potential risk areas and opportunities for improvement. After all, if we don't know it's broken, we can't fix it.

## Recognize Threatening Behavior

The clock is ticking. The risk of a loved one not being treated quickly enough before her condition worsens causes great anxiety for a family member, who begins pacing and becomes increasingly angry (potential risk). Seeing the crowded ED and assuming the staff are too busy to provide immediate attention for his family member triggers the perpetrator to seek immediate medical attention by commandeering staff to assist him (stimulus). An unattended door with a restricted access sign for employees only provides an opportunity for the perpetrator to grab and force a clinician to help now (opportunity to act). Violent behavior erupts, nurses are terrified, and chaos ensues.

The theoretical situation above could have been avoided with proper training and ability to recognize threats early. Understanding how perpetrators behave is key to managing threats. There are some commonalities among individuals who pose a threat. Recognizing threatening behaviors allows resources to intervene at the earliest possible stage.

Most all perpetrators consider, plan, prepare, and then act. This allows intervention at multiple points along the violence spectrum. But effective intervention to decrease threats is dependent on training and experience that enable security officers, public safety, and police officers to fully recognize and identify the early signals. Intervention also relies on nurses and



*This article is excerpted from Chapter 6 of Lisa Pryse Terry's recently published Preventing Emergency Department Violence.*

*continued on page 6*

# The Flexible Security Solution

Implementing best-in-class solutions for high-traffic urban facilities

In preparation for a \$300 million expansion project, Jersey Shore University Medical Center turned to security integrator Service Works, Inc. to design and install a security system that would integrate with equipment already in place. The project, completed in 2009, added a diagnostic/treatment tower, an atrium and a new hospital entrance. Also added were a state-of-the-art emergency department and trauma center, new surgical suites, an expanded outpatient pavilion and a 975-space parking garage.

The hospital relies on access control to protect staff, students and patients. Proximity readers segregate sensitive areas, allowing only authorized personnel to enter the suite of operating rooms. All high-risk areas of the hospital—emergency room, pharmacy, neo-natal department and pediatric intensive care—are covered. As part of the renovation, access control was also incorporated into gates on most levels of the new parking garage.

One important element was the number of people: With the expanded capabilities of the new emergency department, annual visits to that facility have increased to 90,000. With unhindered accessibility and hundreds of individuals coming and going each day, keeping track of that many was a major challenge.

“We also had to consider our urban location,” said David Brooks, corporate director of risk management. “Because we’re serious about protecting everyone on campus, we wanted the ability to lock down the trauma center with one keystroke.”

From the beginning of the planning process, hospital officials sought an access control solution that would integrate with the CCTV and infant abduction systems already in place. “We were looking for a non-pro-



prietary system,”

said Brooks. “We

wanted to avoid the problem of having to call a different vendor every time we needed something.” After examining all the options available from various security providers, they decided to install Honeywell’s Pro-Watch® Corporate Edition security management system because it works seamlessly with third party systems.

## Honeywell

The security system ensures flexibility when issuing badges. Thousands of badges have been issued to staff, emergency vehicles, medical students and volunteers. Hospital officials decided on a standard proximity card for team members and doctors, and a medallion that affixes to the existing magstripe badges carried by students and volunteers. According to Brooks, it’s cost effective and easier to stick a medallion on an existing badge. “That’s the beauty of the system—it’s easy to update readers and change access to existing cards,” he said. Overall, feedback about the new system has been overwhelmingly positive.

For more information contact:

Honeywell Security

800-323-4576

[www.honeywellaccess.com](http://www.honeywellaccess.com)

healthcare staff understanding the signs of pending violence.

Nursing by nature requires staff to be physically close to patients who can quickly become agitated or violent. Close contact increases the likelihood that a nurse or other clinician will become the victim of physical violence, especially if the signs of violence are not recognized early. This increases the need for clinical staff training on the violence spectrum as well as related security training, de-escalation techniques, and personal safety training.

A collaborative effort and integrated training for healthcare security staff and clinicians increases safety for everyone. It also helps define roles and responsibilities if an event occurs. Collaboration reinforces what to expect if an event occurs and how resources can be quickly assimilated.

Security and healthcare staff who are able to proactively deal with threats and/or threatening behavior early—detecting threats early, evaluating them, and knowing how to address them—may be the single most important key to preventing and managing violence.

So how do security and healthcare professionals identify the signs to decrease threats? All staff should be trained on the components of anger and impending violence, which present in three primary ways:

1. Physical reactions—These reactions include an individual's response to anger, frustration, and potential violence such as an adrenaline rush, increased heart rate and blood pressure, and tightening of muscles for the “fight or flight” response.
2. Cognitive experience—This involves how an individual perceives he or she is being treated. If he believes he is being treated unfairly, prejudicially, or in any negative way, the risk of becoming angry and violent escalates.
3. Behavior changes—Individuals considering a violent action or response will display behavioral changes such as change in demeanor, verbal or voice changes, and nonverbal cues of agitation and frustration

such as tapping fingers, rapid eye movement, or pacing. Security and healthcare staff must understand the significance of verbal and nonverbal cues. Key threat management strategies focus as much on nonverbal communication as they do on verbal communication. According to various researchers, body language is thought to account for between 50 to 70% of all communication. Consider the following non-verbal signals:

- In a crowded waiting area, a family member feels claustrophobic and becomes agitated
- A worried parent continually reaches out for the nurse's arm in hopes of getting more attention
- An agitated spouse paces back and forth in front of the doors leading to restricted treatment areas
- The eyes of a frustrated patient dart back and forth continually
- An anxious spouse believes it is taking way too long to get an updated report on his wife and begins clenching his jaw
- A forensic patient visually scours the treatment room for a weapon of opportunity

These are all signs of potential violence. Space, touch, body movement, and perception of time are all ways people express their frustration and anxiety. Proactively identifying these particular behaviors of concern can help reduce the risk of violence in the ED and contribute to a better patient experience. ■

---

*Lisa Pryse Terry*, CHPA, CPP, is a member of the ASIS International Healthcare Security Council and Director of Hospital Police and Transportation at UNC Hospitals.

*Reprinted with permission. Copyright 2014. HCPro, a division of BLR. For more information, visit <http://hcmarketplaces.com/preventing-emergency-department-violence-tips-tools-and-advice-to-keep-your-facility-safe>*

# Networked Access Control Meets the Need

## Healthcare Security Solutions Provide Model for Access Control

As healthcare facilities continue to provide quality care for those in need, they also face the increasing challenge of keeping their facility, resources and staff secure. Being responsible for the security of others is never an easy task. With threats emerging from any number of sources, healthcare administrators and security personnel are consistently being challenged in new ways and continue to search for solutions to a growing number of security concerns.

As a result of this, more and more healthcare administrators are turning attention to Keyscan access control systems as part of their security plan. Our engineers constantly strive for excellence developing new and feature-rich products that offer best-in-class access control solutions. These innovations have resulted in over sixty-five thousand active systems operating worldwide.

In Chicago, Hartgrove Hospital selected a Keyscan system as part of a security plan for their facility. Prior to adopting the Keyscan system, traditional keys and key switches were used. The decision to install a Keyscan access control system eliminated the need for keys by issuing individual card credentials to all staff. With access levels and permissions programmed into the Keyscan software, the system controlled access to all secured rooms or resources. And, if a credential was ever lost, stolen or misplaced it could be removed from the system in seconds ensuring all secured areas remained secure.

Keyscan's system-wide reporting capabilities also served as a great resource. The Keyscan system generated detailed reports that provided useful investigative information to help administrators "fill in the blanks" of who, what, when and where.

For Williamson Medical Centre in Frank-

lin, TN, Keyscan's engineering team helped create a customized integration platform between the hospital's infant security system and the access control system. The floor was equipped with a lock down feature. If an infant was taken toward any exit or elevator the infant alarm sounded and the entire floor was entered into a system-initiated lock down. Only emergency responders had in and out privileges to carry out their crisis protocol.

Keyscan's access control systems are actively used around the world securing hospitals and medical centers as well as embassies, military bases, power generating facilities, automobile dealerships, banks, schools, multi-national organizations, retail establishments as well as many other small, medium and large scale businesses. Now with Keyscan as a member of the Kaba Group, our horizon has broadened significantly. With access to Kaba's high quality access management solutions we are, more than ever, well positioned to provide innovative solutions in the networked access control marketplace.



A Member of the Kaba Group

### For more information contact:

James Duff, Marketing Manager,  
james.duff@kaba.com  
1 888 KEYSKAN



## Enterprise-wide Identity Solutions

Biometrics correctly identifies patients, staff and visitors for efficient and secure healthcare operations. SRI's iris biometric-embedded enterprise tablet offers a cost-effective way to bring accuracy and convenience to existing workflows. This mobile solution enables patient authentication, electronic health record flow, access control, workforce management and other emerging applications.

SRI International's biometric identity solutions can help:

- Protect patient identity**
- Reduce administrative errors**
- Manage physical and logical access**
- Mitigate insurance fraud**

Convenient. Accurate. Secure.

Together, we can integrate biometrics and enhance your healthcare operations.  
Contact us to discuss.

[info@sri.com](mailto:info@sri.com) | 609-734-2553 | [sri.com/iom](http://sri.com/iom)

For product info #44 [securitymgmt.hotims.com](http://securitymgmt.hotims.com)