June 2012 Vol. 8, No. 6

HEALTHCARE SECURITY ALERT
Supplement to Briefings on Hospital Safety

IAHSS releases security design guidelines

New guidelines provide resource for security directors and design teams during building and renovation

Security directors who feel out of the loop when it comes to building and renovation projects finally have a resource to lean on.

In March, the International Association for Healthcare Security and Safety (IAHSS) released *Design and Renovation Guidelines for Healthcare Facilities,* with security-specific guidance for projects ranging from new facility construction to renovation of high-risk areas of hospitals, including the ED, pharmacy, and infant and pediatric units. ("See IAHSS General Guidelines" on p. 3 for an excerpt of the official guidelines.)

The hope is that this guideline will encourage security and safety leaders to inject themselves into the planning stages of building and renovation projects, and encourage architects, designers, and other healthcare leaders to take a closer look at how their blueprints will affect hospital security, says **Tom Smith, CHPA, CPP,** director of hospital police and transportation at UNC Health Care in Chapel Hill, N.C., and task force chair for the IAHSS guidelines.

"What I've seen happen in some cases is people don't really start thinking about security seriously until shortly before or after a new facility opens, and they start putting locks on the doors thinking about how they are going to secure the place at night when no one is around," Smith says. "Or they build the stairwell in the wrong place, so we have to leave areas open so people can get to the emergency exit because of *Life Safety Code*® requirements."

The guidelines should also give everyone involved in new construction or renovation projects the knowledge and confidence to feel they can effectively contribute to pre-construction and design meetings and integrate security features into their projects, says **Evelyn Meserve, CHPA,** executive director of IAHSS.

"The guidelines are written to provide the basic information required to allow security to be proactive during the design or renovation process," she says. "By bringing the guidelines to the table at the initial stage, security will be at the forefront of the thought process throughout the project."

> **"By bringing the guidelines to the table at the initial stage, security will be at the forefront of the thought process throughout the project."**
>
> *—Evelyn Meserve, CHPA*

Talk the talk

Sometimes simply knowing design terminology is half the battle. The IAHSS design guidelines help break down specific security concerns for each unit and how they relate to building plans.

"Some security directors or end users on the design team are unfamiliar with the lingo and less likely to interject themselves to advocate for reasonable security features," Smith says. "Our hope is they can tear off a page of these design guidelines and use the principles set forth to develop their own elements of security and safety in each project."

The general guideline (see p. 3) sets an overall tone for security design issues that may come up during any project. Each subsequent chapter delves more into the specifics of renovations to EDs and other high-risk areas.

For new building construction, the guidelines address issues related to parking and the external campus

environment and then move into buildings and the internal environment.

Get involved early

The key to effectively using the building and design guidelines is to incorporate them early on in the process. When security gets involved late in a project, too many issues are already overlooked, and the hospital ends up paying for them in the long run.

"It's so much less expensive if it's designed in rather than retrofitting it," Smith says. "It's good to put the security features in early on, rather than wait until the building is up and open."

Getting involved early as a security director often means getting invited to design meetings. Smith recommends photocopying chapters of the IAHSS guidelines and sending them to clinical leaders on each unit. Even if there is no current renovation happening, being proactive increases the chance that they will think about including security when the time comes.

"Initial awareness of security in the early stage provides tremendous benefit to the facility and the security department," Meserve says. "The awareness varies at different facilities, but I believe the guidelines will be a resource document that helps improve the consistency of awareness at all levels."

Building relationships with key unit leaders and department heads will also help during the value engineering period, Smith says. During this period, clinical leaders and medical directors sometimes fail to differentiate between wants and needs. If they favor a particular feature over security, security will most likely be trumped in the final plan.

"What I find most of the time is that it's just that they aren't thinking about it," Smith says. "Of course they want security. The clinical staff—especially in the security-sensitive areas like the emergency department, behavioral and mental health locations, and the pharmacy—they want to keep themselves safe. It's just that when you're designing it, that's when you have the opportunity to remind them."

Avoid costly mistakes by doing it right the first time

Smith has heard dozens of horror stories about hastily built facilities that turned out to be access control nightmares as a result.

For example, he recalls one tale about an eight-story healthcare building whose elevators and emergency exit stairwells were configured such that occupants had to walk through clinical areas—areas that were meant to be secured during nonbusiness hours and not meant to be used as a public throughway during normal business hours. This was a fatal security design flaw that resulted in thousands of dollars of retrofitting.

"Here was an eight-story building attached to a major medical complex and you can't lock the doors when the staff go home at five o'clock," Smith says. "It's a simple thing like that where it costs a lot of money to retrofit and provide a reasonable level of security at a later date."

These mistakes usually happen because design and operations leaders are thinking more about work flow and aesthetics, rather than what happens during nonbusiness hours. Security directors can offer their unique perspective to avoid a situation that creates a financial burden down the road. ■

IAHSS General Guideline

Statement: Acts of violence, the potential for crime and terrorism, and the response to and mitigation of emergency incidents are significant concerns for all Healthcare Facilities (HCFs). A consideration of these concerns in the design of new or renovated HCFs presents an opportunity to implement and integrate security design elements that address the delivery of patient care services in a reasonably safe and secure environment, and allows for the cost-effective integration of security applications in architectural, engineering, and environmental design.

Intent:

a. The IAHSS Security Design Guidelines are intended to provide guidance to healthcare security practitioners, architects, and building owner representatives involved in the design process in order to ensure that these best practices are considered and integrated, where possible, into each new and renovated HCF space.

b. This General Guideline establishes a background and framework for subsequent guidelines covering specific areas of vulnerability and should be utilized as a frame of reference and underpinning for incorporating appropriate security features into the design of all new construction and renovation projects. These guidelines include reference materials that provide further detailed subject matter elaboration.

c. The initial planning and conceptual design phase of all newly constructed or renovated HCFs should include a security risk assessment conducted by a qualified security professional.

d. The size, complexity, and scope of services provided within an HCF can vary significantly. Security design considerations should be risk appropriate for the environment and function, while maintaining design consistency across the HCF. Design considerations should support patient care, provide a positive employee and consumer experience, proactively mitigate risk, and address real and perceived security concerns.

e. The development or continuation of institutional design standards related to the protection of vulnerable patient populations, the securing of sensitive areas, the application of security and safety systems—as well as the infrastructure required to support these needs—are issues best addressed early in the design process to be most cost-effective.

f. The design of HCFs should include consultation with the organizational security representative to identify, design, and provide protective measures. The project design team should prepare and submit plans to the project security representative for review and approval, including a comprehensive security plan that indicates a layered approach. This plan will include zones, control points, circulation routes, and physical security technology locations, and should be reviewed by the security representative prior to submittal to the planning, regulatory, and approval authorities. Integrating these design considerations into the development of submittal documents and through the commissioning process will help avoid costly security and safety retrofits.

g. The integration of these guidelines should be in collaboration with the entire design team. Design considerations should coordinate the security plan, the building Life Safety plan, and the regulations that have jurisdiction in the local environment. This type of coordination will ensure egress paths do not access areas of lower security through areas of higher security.

h. Security requirements for construction, commissioning, and move-in will vary according to the complexity and scope of services provided. A security project plan should be developed that is risk appropriate for the environment and function and should include:

- The impact of demolition and phasing of existing site functions and protection efforts.
- The need for temporary security barriers such as fencing and security systems, including intrusion and video surveillance.
- The installation of security systems should be scheduled for completion to allow for protection of the facility and equipment during early move-in activities.

i. An HCF's surroundings may include open space, parking facilities, and private ways, and may border other businesses, residential properties, major transportation routes, or other areas. The design of HCFs related to site planning is addressed within the *Parking and*

IAHSS General Guideline *(cont.)*

External Campus Environment Design Guideline.

j. HCFs provide care to patients in both inpatient and outpatient areas and may include non-patient care areas such as academic and research space. These areas may present specific risks or security concerns and the design of HCFs related to these types of areas are addressed within the *Buildings and the Internal Environment Design Guideline.* These areas, which are addressed in specific design guidelines, include:
   - Inpatient Facilities
   - Emergency Department
   - Mental Health Areas
   - Pharmacies
   - Cashier and Cash Collection Areas
   - Infant and Pediatric Facilities
   - Protected Health Information Areas
   - Utility, Mechanical, and Infrastructure Areas
   - Biological, Chemical, and Radiation Areas

k. HCFs frequently provide both scheduled and emergency services, serve as part of local emergency response networks, and are frequently expected to be functional, safe, and secure for patients, visitors, and staff while remaining prepared for natural and man-made emergencies 24/7. The design of HCFs related to these types of issues is addressed within the *Emergency Management Design Guideline.*

l. The development of the Security Design Guidelines for Healthcare Facilities reflects the principles of Crime Prevention Through Environmental Design (CPTED). These principles, when applied early, can be integrated into any HCF design providing layers of protection for patients, visitors, and staff.

m. CPTED defines territories and how they are controlled and managed based on the use of "concentric rings of control and protection." Outermost rings are supported by additional inner rings of protection. Each of these concentric rings will be addressed as layers of protection within these guidelines and are intended to sequentially deter, deny access to, and slow down possible malefactors. In the healthcare environment, CPTED layers may include:
   - The first layer of protection should be at the perimeter of the property, which limits points of entry. The campus perimeter should be defined by fences, landscape, or other barriers. At certain locations, this may include the building exterior. Campus entry points should be controllable during emergency situations or heightened security levels.
   - The second layer of protection should be at the building perimeter and consist of doors, windows, or other openings. Protective elements or components may include access-control hardware, intrusion detection, video surveillance, use of protective glazing materials, or personnel for control and screening at selected entrances during designated times.
   - The third layer of protection should be inside the building itself, segregating authorized and unauthorized visitors. Using physical and psychological barriers and hardware, this layer is most frequently applied in areas of higher risk such as emergency treatment areas, intensive care units, mental health areas, pediatric units, newborn nurseries, and recovery rooms.
   - The fourth layer of protection should segregate generally accessible public and patient areas and staff-only areas. Using physical barriers and locking hardware, this layer is most frequently applied to areas that restrict all visitors and limit access to HCF staff only in areas such as nursing offices, staff locker rooms, storage and distribution locations, food preparation, sterile corridors, and research laboratories.
   - The fifth layer of protection should further restrict staff access to highly sensitive areas. Using physical barriers and locking hardware, this layer is most frequently applied to areas that are limited to vetted and authorized HCF staff. These areas frequently include the pharmacy and narcotic storage spaces, hazardous materials, plant utility and information technology infrastructure, and areas housing personal health information (PHI). Security design considerations for such areas should be addressed in accordance with applicable regulatory oversight, standards, and guidelines.

Source: Security Design Guidelines for Healthcare Facilities, *IAHSS. Published 2012. Reprinted with permission.*