Use IAHSS guidelines to design your hospital security plan

Editor's note: This guest column was written by ***Thomas A. Smith, CHPA, CPP,*** *president of Healthcare Security Consultants in Chapel Hill, N.C. He currently serves on the International Association of Healthcare Security and Safety (IAHSS) Guidelines Council, the Facilities Guidelines Institute Health Guidelines Revision Committee, and the ASIS Healthcare Council. Smith has previously served as director of hospital police and transportation at University of North Carolina Hospitals in Chapel Hill, and chairman of the IAHSS Healthcare Security Design Guidelines Task Force.*

Designing security features into new or renovated space from the beginning can improve safety and security, maximize utilization of human resources, and lower operational costs while improving customer service, and employee and patient satisfaction.

Using the IAHSS security design guidelines can help you assemble an effective hospital security plan. Visit *http://iahss.org/About/Guidelines-Preview.asp* to download the guidelines.

It can be easy to miss or glaze over meaningful discussion about security in the early stages of design. Often the design team and unit leaders are so focused on designing their new space that security is not seriously considered until major decisions already have been set in stone. These include stairwell location, traffic patterns, and adjacent functions that may lead to conflicting operational needs, such as placing a night food service operation inside the nighttime perimeter of the facility, which would require additional security checkpoints.

When security flaws are designed into a project, expensive change orders and retrofitting usually are necessary. Sometimes it is impossible to alter a design due to conflicts with life safety codes or cost-prohibitive retrofitting expenses. Add-on security features also may deter from the aesthetic value of a project, and the final project may end up costing a great deal more.

The worst case occurs when appropriate security features are left out, or are value-engineered out, and an adverse incident occurs. This can result in adverse public scrutiny and erosion of confidence in the healthcare facility by its patient and employee base. At this point, the security features are added at great expense. Retrofitted security features are almost always more obvious and less effective than security features that are designed in at the early stages.

General guidelines

This section lays the foundational security and design principles that are carried throughout the remaining guidelines. It establishes the principles of risk assessment and the inclusion of an assigned project security representative, as well as the concepts of protecting in layers through the creation of concentric rings of control and crime prevention through environmental design (CPTED). All succeeding sections complement the security design elements in the general guideline.

- **Parking and the external campus environment.** This guideline complements the general section through expansion of principles relating to CPTED and establishment of the first ring of protection at the property line. Additional concepts that receive elaboration include the use of physical barriers; coordination of vehicle entrances; landscaping and pedestrian walkways; surveillance and lighting systems; access control principles at the perimeter to reduce the potential for unobserved pedestrian access by channeling access; using natural barriers or fencing; transit placement; lighting and wayfinding; and parking facility security considerations.
- **Buildings and the internal environment.** With nine subguidelines, this guideline is the most voluminous and defines zones of protection within the internal environment; management of access systems; and areas requiring such special security consideration.

The typical zones in the healthcare environment include general areas accessible to the public at all times (i.e., lobbies, EDs, and entrance points), general areas restricted to the public during non-visiting hours or periods of lesser activity (i.e., restricted waiting rooms

and closed departments), screened public areas, staff and accompanied public areas (i.e., operating room recovery areas), general staff-only areas, and areas for designated staff with the appropriate clearance.

The operating procedures for access systems and the type of systems specified should be consistent across the healthcare facility. Electronic security systems, if available, should be integrated and standardized. A few of the design considerations in this guideline include alarm points, closed-circuit television, door hardware security requirements, wayfinding and signage, and coordination with other building technology systems.

Areas requiring special consideration (excluding designated security-sensitive areas) are identified in this guideline. They include materials management; central supply and sterile processing; shipping and receiving; mailrooms; health information management and medical records; human resources; administrative and business offices; meeting rooms and conference areas; call centers, switchboards, or other staffed telephone answering centers; research facilities; child care centers; urgent care facilities; and operating rooms, sterile areas, and special procedures areas.

Inside your facility

Subguidelines within the buildings and the internal environment guidelines largely concentrate on locations whose function or activity presents an environment in which there is a significant potential for injury, abduction, or security loss that could severely impact the ability of the organization to render high-quality patient care. They include the following:

- **Inpatient facilities.** This guideline complements the earlier guidelines by further elaborating the concepts of protection in layers, including zones, control points, circulation routes, and required egress paths. Major points of emphasis for this guideline include placement of elevators and stairwells to avoid conflicts between life safety and security. It also features design considerations for reception areas, information desks, and other customer service or screening stations.
- **EDs.** The ED should be viewed as a secured area providing an added layer of protection between the healthcare facility, public areas, and treatment areas. The project design team should develop a comprehensive security plan that indicates a layered approach including zones, control points, circulation routes, and required egress paths. Detailed elements of this guideline include recommendations concerning adjacent spaces, parking, and a distinction between internal and external ambulatory and non-ambulatory access points. Other highlights of this guideline include recommendations relating to waiting rooms, weapon storage, patient valuables, furniture, security and police work stations, high-risk patient observation rooms, and prisoner patient rooms.
- **Behavioral/mental health areas.** Behavioral/mental health (BMH) patients pose unique challenges and risks as a result of their medical condition. The BMH guideline provides guidance for stand-alone facilities and units within larger medical complexes. It offers detailed recommendations relating to perimeter design, internal space, and safety and security systems.
- **Pharmacies.** The design of pharmacies should address the unique risks presented by the storage and distribution of narcotics and other controlled substances. The design should create a secure physical separation between pharmacy operations and the public while integrating security systems for access and audit functions. Specific intents within this guideline provide recommendations concerning physical security, protection of people, and audit capabilities.
- **Cashiers and cash collection areas.** The collection, storage, and handling of cash presents unique security risks to healthcare facilities. Security design considerations for primary and secondary cash collection areas should integrate the physical location and layout with security controls and technology. The risks posed by cash collection primarily involve robbery and internal theft. This guideline provides specific measures covering safes, physical security, video surveillance measures, and audits.
- **Infant and pediatric facilities.** Infants and pediatric patients are vulnerable patient populations requiring added security measures and special attention when designing a space. Design team members should consider the patient and family experience, the physical location and layout, and integration of security controls and technology. Intents within this guideline provide recommendations for reception and waiting areas, access control zones, circulation routes, physical security, and technology. Other special areas of consideration

include security elements for the new-mother rooms, infant monitoring, and pediatric play areas.

- **Areas with protected health information.** Guarding protected health information is an important element of any health facility renovation or new construction project. Designs should address the multiple ways in which privileged information could be compromised and should protect that information by utilizing integrated physical and electronic security systems. This guideline relates to signage, registration areas, furnishings, equipment locations, video surveillance, and waste.
- **Utility, mechanical, and infrastructure areas.** The design of facility utility, mechanical, and infrastructure-related space should include the recognition that such space and the mechanical, electrical, plumbing, and information technology systems within it are critical assets for the facility. The systems typically housed in these spaces are essential for uninterrupted patient care, basic building comfort, and emergency response capabilities. This guideline is intended to provide recommended security design elements for utility systems, mechanical and infrastructure spaces, and built-in redundancy and expansion capabilities pertaining to technology and mechanical systems.
- **Biological, chemical, and radiation areas.** Healthcare facilities must address the unique security risks presented by highly hazardous materials, including but not limited to biological, chemical, and radioactive materials. These materials frequently are regulated, and areas must be designed accordingly. This guideline provides recommended design elements covering spaces to be addressed, waste streams, emergency response, and audit features.
- **Emergency management.** The final major area of emphasis is emergency management, which recommends that health facility designs consider practices that allow for flexibility and resilience required to manage emergency events.

An "all-hazards" approach to design should be applied to help the facility prepare for, respond to, and recover from man-made events and natural disasters alike. This guideline provides recommendations relating to designs that support sheltering in place and repurposing space during emergency operations to accommodate intake and care of a surge of patients.

Designs should facilitate alternative points of access, space reassignment, emergency access to technology infrastructure, a lockdown of spaces, and designation of space to provide services to support large numbers of individuals in areas separate from patient care and emergency management.

Using the guidelines

These guidelines are meant to encourage leaders in planning security, safety, and emergency management features into building and renovation projects and to incorporate effective security concepts at the earliest stages of design. The guidelines should give everyone involved the knowledge and confidence to effectively contribute to preconstruction and design meetings. Moreover, these guidelines easily could be adapted to internal facility guidelines and used as a template for creating a minimum design standard for projects.

The bottom line is that these design features, when properly applied, will result in reduced cost, improved employee and patient satisfaction, and increased safety. By reasonably addressing security risks up front and early on during design, organizations can cost-effectively address the safety and security of new or renovated space. These steps will help reduce the potential for security features either not being designed into new space or added on as an afterthought, or becoming "value engineered" out as projects face limited budget dollars. The intent of integrating these guidelines early in the design process is to emphasize the importance, incorporate the work into other aspects of the project, and ultimately avoid expensive change orders, retrofits, or other liabilities incurred by the omission of appropriate planning for a safe and secure environment.

It is our hope that healthcare security and design professionals use these design guidelines for every renovation or new construction project. Healthcare facilities may also develop organizational standards for design based on these standards. We also recommend that security professionald at healthcare facilities use these guidelines as a basis for discussion with their design staff and customer base. For example, the design guideline covering the ED can be used as a stand-alone guideline and should be forwarded to the department head or manager responsible for that area as a basis for future renovation or creation of new space.