Hospital Security: The Past, The Present, and The Future, Part 2 of 2

Healthcare security consultant Jeff Aldridge examines the need of risk assessments and the hospital security management plan

Jeff Aldridge, CPP
SecurityInfoWatch.com

Jeff Aldridge, CPP, is a nationally known expert on hospital security and a regular contributor to SecurityInfoWatch.com.

[**Editor's note:** This featured column is the second part of a regular series of columns on healthcare security. Author Jeff Aldridge and others from Security Assessments International have agreed to discuss the changing needs of security in hospital settings, and will be addressing new technologies, procedural changes and new issues affecting today's healthcare facilities. Look for these articles to appear each month on our Healthcare Security section, as Jeff and his associates begin this in-depth review. To read the first part of this article, which appeared last month on SecurityInfoWatch.com, **click here**.]

Security Management Plan

The written Security Management Plan (SMP) is designed to provide a proactive approach in the protection of patients, visitor, staff, and Health System assets. This is accomplished by identifying security threats in all areas of the facility which could have an adverse impact on persons and property.

This is accomplished through the security assessment which is also designed to reduce the occurrence and severity of security incidents and promote security education and training for hospital employees and staff.

Elements of the Security Management Plan

1. Develop, implement, maintain and evaluate a comprehensive facility wide Security Management program.
2. Identify, develop, implement and evaluate written policies and procedures that are designed to enhance security.
3. Assist Department Managers in the development, implementation and review of departmental security policies and procedures.
4. Promote and maintain an ongoing hospital wide hazard surveillance program to detect and report security hazards related to patients, visitors, staff and property.
5. Establish a system for reporting security occurrences and security hazards which involve patients, visitor, staff, and property to include a mechanism for the investigation, documentation, and review of security incidents and actions taken.
6. Review and monitor data to present to the EOC Committee for the purpose of identifying trends and measure the effectiveness of the SMP on an annual basis.
7. Maintain current reference documents and publications related to health car security, including federal, state, and local regulations and resources provided by various regulatory and private agencies which impact on the healthcare system.
8. Be familiar with regulations and resources provided by the various regulatory and private agencies that regulate healthcare facilities.

9. Implement, train, and monitor propriety of security staff charged with enforcing the hospital’s security policies, protocols, and procedures.
10. Develop policies and procedures for the Security Department to assure the Plan enhances the overall security operations of the facility.
11. Nurture and maintain a positive relationship with all regulatory and enforcement agencies, which may impact on the healthcare system.
12. Provide an identification system appropriate for employees, staff, vendors, and visitors.
13. Provide access control to various areas within and on the hospital grounds to include access control to sensitive areas in the hospital as deemed appropriate by the institution.
14. Maintain the facility Parking Plan to include patient, visitor, and staff access to the facility. The program should include traffic control at sensitive location such as the Emergency Department. All parking rules and regulations should be enforced.
15. Cause the removal of person(s) and up to the arrest of anyone committing a crime or cause the necessary action to be taken for non-compliance of the hospital’s policies and procedures as direction by Administration.
16. The Director of Security will develop an annual evaluation of the SMP through a security assessment to determine effectiveness of the plan.

The hospital security assessment should evaluate a facility beginning in the parking lot and continue all the way to the roof. Some of the components that should be considered are:

- Geographical Location (Inter-City, Suburb, Rural)
- Physical Design and layout of campus and surrounding property
- Number of uncontrolled access points into and out of the Facility
- Criminal Demographics surrounding the hospital and campus
- Security Incident data within the hospital as well as incidents on campus
- Level of physical security protection.
- Previous Security Sentinel Events
- Quality of the Security Department and Security Management Program
- Employee Security Awareness associated with on-going educational programs
- Administration and Management Support
- Patient, Staff, Employee, vendor, and visitor identification
- Emergency Department Security
- Violence in the Workplace issues, (Clinical and other locations)
- Birthing Center Security
- Pediatric Security
- Pharmacy
- Employee Education
- Patient Education

Security Sensitive Areas

The Joint Commission requires that healthcare facilities identify security sensitive locations within the hospital that may require unique security protection. Sensitive locations require special training, additional physical protection, and policy / procedures specific to the location identified.

Sensitive locations include, but may not be limited to:

- Birthing Center (Maternity, Nursery, L&D, Postpartum)
- Pediatrics
- Emergency Department
- Psychiatry (Inpatient)
- Psychiatry (Outpatient)
- Radiation Therapy
- Nuclear Medicine
- Pharmacy
- Medical Records
- Information Services

- Human Resources
- Surgical Services (Operating Room)
- Food Services

Physical protection may include but is not limited to:

- CCTV
- Time delay lock & alarm system
- Panic Alarms
- Special Locks
- Protective Barriers
- Security Presences
- Dedicated Security Patrols

Unique policies include, but may not be limited to: access control, visitation, identification procedures, information security, and patient privacy.

Sensitive areas should identified with a Risk Value Rating 1-5, where:

1 = No Risk or not applicable
2 = Minimal Risk
3 = Moderate Risk of Injury / theft
4 = Significant Risk without history of injury / theft
5 = Significant Risk with history of injury / theft

Access Control

We have already established that, for the most part, criminal assaults which occur within our hospitals are perpetrated by persons not authorized to be there. Access control is designed to insure that only authorized persons are allowed to enter and leave the hospital. It is imperative that everyone having a legitimate reason for requesting entry into a hospital be appropriately identified. By the same token, controlling access out of the hospital is just as important. For example, infant abductors have been granted access into hospitals as authorized visitors, but after abducting a baby they escape capture by NOT using authorized / controlled exits. Unauthorized persons perpetrating other acts of crime in hospitals including criminal assaults, rape, murder, and theft will immediately look for the closest escape route, which is usually an unlocked emergency egress.

The public should be educated and directed to use an entrance that is dedicated to patients, visitors, and guest. A separate entrance should be dedicated to employees and staff. Control all employee, staff, and doctor entrances using card access. Issue a visitor's badge to visitors, contractors, volunteers, and students. Require the vendor's badge to be returned and the vendor to sign-in and out of the facility.

Emergency Egress /Locks & Alarms

Don't forget it's just as important to prevent unauthorized egress from the facility as it is to prevent unauthorized access into the facility. An uncontrolled, unlocked emergency exit provides an escape route for a fleeing criminal. Uncontrolled, unlocked exits also encourage patients to leave the hospital against medical advice (AMA). The National Fire Protection Association (NFPA) 2000 Edition permits door-locking devices with delayed egress in healthcare occupancies, or portions of healthcare occupancies. The code states that where the clinical needs of the patients require specialized security measures for their safety delayed egress is acceptable. The delayed egress hardware is designed to lock and alarm for fifteen seconds before allowing an individual to exit. In the event of fire the delayed egress locking system is over ridden by the facility fire alarm protection system. The fire alarm protection system has priority over all other systems and will automatically unlock all emergency exits in the event of a fire. Delayed emergency egresses serve as a deterrent to individual that may target the facility. Card access can be provided both for egress and ingress.

Camera/CCTV Surveillance

Many of the CCTV surveillance cameras and monitors in use in hospitals today are the old black and white analog systems which are not state-of-the-art products and are obsolete. Many of the cameras are not equipped with recording capability and may be positioned incorrectly. Several systems currently in use by hospitals are not monitored and are in disrepair and non-functional. In many cases hospitals do not have a Central Security location provided to monitor, record, and dispatch security response to security events that occur in their facility.

Hospitals need to replace obsolete CCTV surveillance systems and upgrade to a state-of-the-art digital, color, matrix system with digital archiving capability. Cameras should be installed in security sensitive locations such as public entrances, parking locations, entrance and exits, as well as sensitive areas such as the, Birth Center, Emergency Department, ATM Machine, Loading Docks, Cashiers, and Pharmacy. The CCTV system should also be integrated with access control through the hospitals IT infrastructure.

Photo I.D. System

A large number of hospitals still continue to use old hospital identification cards that do not display the employee's photo. To my absolute amazement, a few are still using the plastic name tag with just the employee's name displayed on the tag. Any office supply will be glad to sell you a bucket full with any name you would like to have engraved on the tag. More alarming is the fact that many hospitals do not enforcement the wearing of any type of hospital identification by employees and staff. Every employee and staff member, including doctors should be required to wear a tamper-proof photo identification badge, facing, forward, displaying the person's first and last name, title, and the hospital's name and logo.

Hospitals that fail to require all employees and staff to display a photo identification badge are exposing themselves to serious litigation. Several years ago I testified as an expert witness in a case where a hospital was sued for several million dollars because the hospital did not require all of their employees to wear Photo I.D. badges. An infant was taken from the nursery by an abductor thought to be a fellow employee by a new staff member. Photo I.D. badges were not required to be worn in the nursery because staff had complained that the I.D. badge scratched the babies when they were being held. Facilities need to replace their out-dated I.D. systems with a state-of-the-art computerized photo imaging system where the photo is implanted into the PVC plastic card.

This type of I.D. system offers many advantages. For example, this type of system archives the image so that it can be used to make a replacement badge for an employee without the employee having to leave his or her work area to have another picture taken. Many hospitals have incorporated a bar code or smart chip into the card to provide time and attendance for their employees as well as being able to restrict access to certain locations for unauthorized employees.

Emergency Department Threats

A Justice Department study reveals that hospital emergency departments across the country treat more than 1.3 million people a year for injuries caused by violent attacks, an increase of 250 percent over previous government estimates. A study by Erickson and Williams-Evans (2000) reveals that nurses are the frequent targets of assault and the greatest number of assaults (25%) occurred in emergency departments; of the 51 homicides recorded, 23% occurred in emergency departments.

Crime has penetrated into the healthcare setting at an alarming rate. Assaults on medical personnel are becoming increasingly frequent and severe. Emergency Departments across the country are becoming the scene of violent attacks by patients, relatives or their friends, often involving knives and guns. Hostage taking situations are on the rise. And now after the September 11th attack on America, hospitals are beefing up security to prepare for mass causalities in the event of a bioterrorism attack. With these increasing trends healthcare providers are facing serious liability and the charge is usually, with out exception, inadequate security.

Patients are being found in possession of knives and guns on a daily basis in the patient treatment areas of our Emergency Departments. Weapons need to be detected before they enter the patient treatment area of our Emergency Departments. Metal detection and scanning are the only methods for detecting unauthorized weapons brought illegally into the Emergency Department. Hospitals should seriously consider installing a metal detector at the entrance to the Emergency Department to screen all persons that attempt to enter with unauthorized weapons.

Infant Electronic Protection

Concerns about wandering patients and infant abductions have been a common fear among hospital administrators for some time. These concerns have brought renewed interest in electronic tracking of patients and infants. Litigation continues to be brought against hospitals and birthing centers with charges of inadequate protection against infant abductions. As a result, this phenomenon has sparked a myriad of manufacturers and vendors to develop a variety of systems designed to foil abduction attempts and locate wandering patients.

With the continuing increase in litigation and the wrath of the Joint Commission, it becomes increasingly essential for hospitals to offer state-of-the-art security protection for their mother/baby and pediatric units. The proliferation of new security products makes it increasingly difficult for administration, nursing, and security management to select a system that provides the ultimate protection and ease of use at a reasonable cost.

When deciding on an infant security system it is best to form a committee from various disciplines and departments within the hospital. The following link lists some of the evaluation criteria recommended for committee use: **http://www.saione.com/eps.htm**.

IT Security

Whether a hospital implements even a small component of technology to manage EPHI or is a full-scale, automated facility, the 42 HIPAA safeguards must be addressed. IT security means a secure network, secure data transmission and the protection of patient confidential information. This aspect of IT security is now of paramount importance to hospitals and healthcare affiliations because of HIPAA mandates. By assessing the current network environment, deploying technologies that address the exposures uncovered by the assessment, developing appropriate IT security policies and procedures, and validating and maintaining the security solution through real-time monitoring and periodic audits, ensures that the facility has it's IT environment secure.

Proactive management and resource allocation is the only way to keep up with the never-ending changes in laws, regulations, and threats. This is accomplished by maintaining adequate staffing, access control, personnel orientation, continuing education, and the identification of patients, visitors, and staff, all of which is mandated by industry standards.

Prospective patients and families are increasingly evaluating hospitals not only for the quality of care a hospital provides, but now, more than ever, hospitals are being evaluated on the level of security available during the patients stay. With this in mind, it becomes increasingly essential for healthcare providers to offer state-of-the-art security protection for their patients, staff, and visitors.

About the author: Jeff Aldridge is an internationally recognized healthcare security consult and the Nation's "Number One" expert on infant security. Jeff works with Fortune 500 Companies in the design and development of state-of-the-art security products for the healthcare industry. He founded Security Assessments International (SAI is online at **www.saione.com**) in 1994 and continues to provide services for healthcare facilities throughout the U.S. and overseas. In addition, he serves as a consultant to the National media and law enforcement on infant security issues and has provided collaborative assistance to the National Center for Missing & Exploited Children. Over the past 16 years Jeff has assisted over 600 healthcare facilities throughout the U.S. and abroad with their healthcare security issue. Jeff has assisted clients in England, Ireland, Australia, and Kuwait. He has been featured on ABCs 20/20, as well as "PM Magazine", a nationally syndicated television program. He was recently interviewed by NBC, CBS, and the FOX network concerning mother/baby mix-ups in hospitals.

Jeff is a much sought after speaker for national and international healthcare organizations as well as a published author. Jeff testifies as an established expert witness in high profile infant abduction cases. He can be reached by email at **jeff@saione.com**.

Related Stories

- **Hospital Security: The Past, The Present, and The Future, Part 1 of 2**