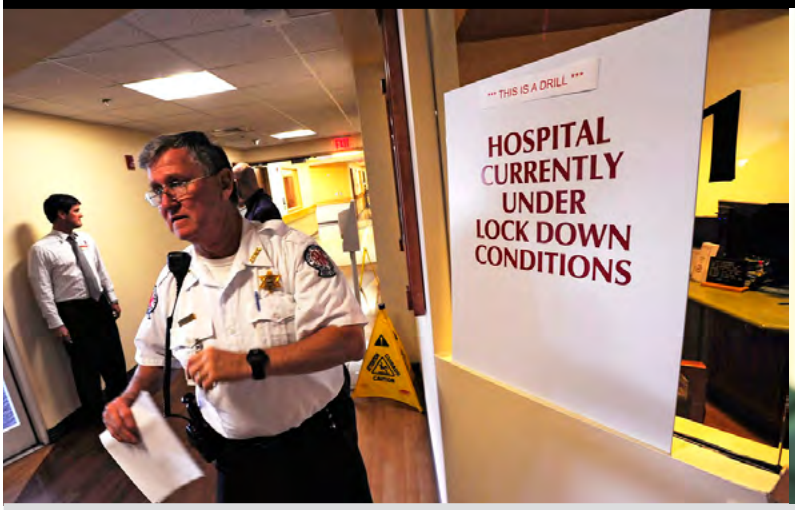
RiskWatch

www.riskwatch.com



Healthcare

Security Risks and Mitigation Strategies

HEAL

This white paper discusses the necessity of a robust security program in healthcare organizations and demonstrates how the identification of security technology can create operational efficiencies. It also illustrates how hospital security teams can manage the balance between protection and openness by conducting a comprehensive risk assessment and developing a hospital security program, and thereby limit the risks to a manageable level.

Introduction

Securing an environment of care and safety in healthcare organizations involves unique challenges of attaining harmony between obviously conflicting factors.

The challenges are distinctive primarily because healthcare facilities must maintain an open environment while at the same time maintaining the desired levels of security, service quality and patient satisfaction. This scenario is ongoing and hospital security managers are finding it increasingly difficult to accomplish a balance between them.

Control over the situation fails as senior management teams responsible for the security are not always fully aware of the necessity laid down by regulations to protect patients, employees, visitors and critical assets all alike. Furthermore, a misguided conception of ignoring the need of a robust risk assessment and Security Master Plan (SMP) leads to neglecting the priority of a comprehensive security program.

This white paper discusses the necessity of a robust security program and demonstrates how the identification of security technology enrichment opportunities can create efficiencies for hospital operation. It also illustrates how hospital security managers can effectively manage the balance between protection and openness, by conducting a comprehensive risk assessment and developing a hospital security program, thereby reduce the risks to a manageable level.

Attaining this objective requires that hospital security managers win the assurance of senior management to enhance security and financial support for implementation. This again necessitates that security managers comprehend the rationale for a technology-based security program and are capable of presenting a cost-efficient action plan. This white paper offers only the informational backdrop necessary to fulfill the objective and calls on security managers to proactively engage in the development a SMP to meet the specific requirements of their facilities.

Hospital Risk Management Areas

The overall security objective of healthcare organizations is the avoidance of liability, primarily legal. However, security strategies in healthcare organizations can be broadly categorized under three risk management areas. They comprise regulatory compliance, safety of occupants, and assets protection.

Regulatory Compliance

Against a backdrop of steadily increasing violence in healthcare facility safety norms, the protection of people and critical assets has gained in prominence. Although hospitals have always proactively intended to safeguard the people and important assets, it is the defining levels of security – implemented or attained – that have been questioned. For any people intensive healthcare business in the U.S. the key security requirement is clearly defined in the Occupational Safety and Health Administration (OSHA) General Duty Clause and tort law. Under the OSHA General Duty Clause employers are responsible for providing "a place of employment which is free from recognized hazards that are causing or are likely to cause death or serious physical harm." The agency has laid down this basic foundation for people intensive businesses to take reasonable measures to safeguard occupants' physical safety. Although OSHA recommendations do not make it a duty for hospitals to protect occupants against criminal attacks, an all-inclusive reasonable care is emphasized.

In the healthcare and social assistance industry sector more number of employees are injured, with work related injuries and illnesses being one of the highest. The Bureau of Labor Statistics (BLS) release for 2010 for the industry reported 152,000 more cases of injury and illness than the next industry sector, manufacturing, with the total being 653,900 cases. For 2012 the number of cases stands at 621,100. Following a BLS report in 2000, which indicated that 48 percent of all non-fatal injuries from violence occurred in a healthcare environment, OSHA published an advisory document in 2004 titled Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers. Identification of inherent risks in an industry where such occurrences are considered exceptions calls for the creation of special duty on the part of healthcare facility authorities to safeguard employees.

Currently, about 77 percent of hospitals in the U.S. are accredited by The Joint Commission (TJC) – formerly the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) – and approximately 90 percent the recognized hospitals are TJC accredited. TJC accreditation makes a strong statement to the public and medical community that the organization is equipped to provide the highest safety and quality care services. The nation's hospitals seek TJC accreditation because the federal Medicare and Medicaid payers require accreditation to be eligible to receive Medicare and Medicaid payments.

Accreditation may improve the ability to secure new business as it provides a marketing advantage in a competitive healthcare environment. Also, being accredited by The Joint Commission helps healthcare organizations position for the future of integrated care. Since TJC is responsible for the accreditation of hospitals, hospital administration must place due emphasis on compliance. TJC accreditation is considered one of the most effective methods of compliance with government medical program reimbursement requirements.

The Joint Commission Environment of Care (EC) is made up of three components: building(s), equipment, and people. Security management goals are also included in one element of the environment of care. To effectively manage the EC organizations must: Reduce and control hazards and risks; Prevent injuries; Maintain safe conditions for patients, staff and visitors; Maintain an EC that is sensitive to patient needs for comfort, social interaction, and positive distraction; Maintain an EC that minimizes

Regulatory Compliance

unnecessary stresses for patients, staff and visitors.

Security compliance standards for healthcare centers include: managing the security of facility occupants, implementing security controls, identifying people entering the facility, controlling access into and out of security-sensitive areas, and implementing infant and pediatric abduction security procedures. TJC standards also mandate implementation of procedures to report and investigate security breaches. It is imperative for healthcare centers to comply with these goals to stay safe against compliance of written declaration and unannounced inspections. To maintain a database of security incidents and investigation records, organizations must use electronic system to analyze data which, in turn, will facilitate to identify incident frequency.

The Joint Commission observed that healthcare centers plan and respond more effectively when accountability for emergency management is assigned to a high level of leadership. This led to the new and revised emergency management standards, which are effective January 1, 2014. The new elements of performance (EP) require the organization to identify a leader to oversee emergency management and consider input from staff when evaluating exercises and responses to events. The senior leadership should review the emergency management planning activities, performance in exercises, and responses to actual events to facilitate improved communication of problem areas and implementation of solutions. The 2008 Joint Commission emergency management standards identified six critical areas to be addressed in order for an organization to effectively manage an emergency response. They include communication; resources and assets; safety and security; staff responsibilities; utilities management; and patient clinical and support activities.

The Joint Commission also directly referred to five other standards: continuity of information; influx or risk of infectious patients; patient flow; granting disaster privileges; and assigning disaster responsibilities.

Organization leadership would be wise to include the concepts in the organization's emergency plans. The 2006 standards included exercising emergency management response plans and capabilities, conforming to priority emergencies identified in a hazard vulnerability assessment, twice a year. To accomplish the requirements facility security must be incorporated to the tests. A robust security technology will enhance an organization's compliance efforts with these standards. It will also considerably eliminate human error chances and augment surveillance capabilities.

In June 2013, the Joint Commission approved a new National Patient Safety Goal (NPSG) on clinical alarm safety for hospitals, to be implemented in two phases: effective January 1, 2014, and January 1, 2016. The first phase requires critical access hospitals to establish alarm safety as an organizational priority and identify the most important alarms to manage based on their own internal situations. Phase two expects hospitals to develop and implement specific components of policies and procedures, and to educate staff about alarm system management.

However, the proposed phase two requirements may be enhanced based on experience with phase one requirements as well as newly emerging evidence about best practices. Despite healthcare improvements related to efforts to meet the NPS goal, adverse patient events continue to occur related to alarm system performance. Clearly, technological support will go a long way in helping analyze adverse event databases and improve the effectiveness of clinical alarms. Also, accelerated deployment of a comprehensive technology will ensure safer and more efficient healthcare delivery.

The nation's hospitals receive funding from the federal Medicare program, which is managed by the Centers for Medicare and Medicaid Services (CMS). Patients covered under this program receive treatment at hospitals who, in turn, seek reimbursement for the services provided. However, attaining eligibility to receive the taxpayer funds healthcare establishments must meet

Regulatory Compliance

the criteria laid down by Title 42 (Public Health) of the Code of Federal Regulations Part 482. The requirements mandate a comprehensive facility security and safety, including a patient's right to: "receive care in a safe setting," "right to be free from all forms of abuse and harassment," be free from "restraints of any form that are not medically necessary," and "procedures for ensuring the confidentiality of patient records". The reimbursement could be suspended due to non compliance with any of these requirements, resulting in financial loss of devastating proportion for the hospital.

The regulations also mandate that the healthcare center be "constructed, arranged, and maintained to ensure the safety of the patient." Drugs are required to be kept in safe storage areas, assessed only by authorized personnel. These requirements may seem clinically oriented, but ensuring these standards in an open access environment can be quite demanding. Therefore, healthcare organizations need to realign their risk management and quality activities.

Further, the U.S. Department of Health and Human Services (HSS) announced enhanced safeguards to ensure privacy of patients' Protected Health Information (PHI) through the Health Insurance Portability and Accountability Act (HIPAA). The legislations require the covered entities to conduct comprehensive risk assessments of medical records security and access, and to implement administrative, technical and physical safeguards. The legislation emphasizes on having a supervised access control system and video surveillance with recording capabilities, to restrict access and to provide a record of access attempts, authorizations, and denials.

Following the catastrophic events of 11 September 2001, the U.S. government has placed exceedingly high emphasis on the nation's critical infrastructures protection. The Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience identifies Healthcare and Public Health (HPH) as one of the 16 key critical infrastructure sectors. Hospital infrastructure systems are basic HPH elements. The 2009 National Infrastructure Protection Plan (NIPP) details various risk assessment and mitigation strategies for the designated facilities in the sector. The NIPP assigned Department of Health and Human Services (HHS) as a Sector-Specific Agency (SSA) to lead the collaborative process for critical infrastructure protection within the HPH sector.

The HHS require hospitals to develop and implement protective programs for key critical infrastructure, recommend minimum security standards, identify best practices and conduct cost benefit analyses for new protective programs. It issues guidance to hospitals regarding appropriate security measures needed to protect facilities and their occupants. Thus hospitals as a critical infrastructure facility require greater protections due to their national significance and the probability that a major incident could cripple the capability to provide essential medical services.

Safeguarding People

Ensuring safety and security of people should be the highest priority of all people intensive care delivery environments, more so for healthcare organizations. Hospital occupants can generally be classified as patients, staff or visitors; however, they are also frequented by types of people including infants and children, prisoners, people with mental disorder, the elderly and frail, celebrities, drug addicts, thieves, and sex offenders. Hospitals must convey the same sense of security to all. Further, healthcare facilities must adopt open campus environment policy to serve everyone in need of care, irrespective of factors that may disqualify them from receiving services in other business facilities. These scenarios require that hospitals politely validate the presence before routing them to the appropriate facility. Therefore, in hospitals preparedness and efficiency are critical components of plan and policy aimed at enhancing the security and mitigating risks, and should be integrated into the overall risk management approach to reduce incidents and liability.

In the U.S. workplace violence is calculated with fatal and nonfatal statistics from numerous sources. The Bureau of Labor Statistics (BLS) Survey of Occupational Injuries and Illnesses (SOII) reported an estimated 130,290 nonfatal occupational injuries and illnesses involving days away from work during the 2003 to 2010 time period. The Healthcare and Social Assistance Industry accounted for 63% of these injuries and illnesses each year. In 2010, BLS data reported healthcare and social assistance workers were the victims of approximately 11,370 assaults by persons; a greater than 13% increase over the number of such assaults reported in 2009. Almost 19% (2,130) of these assaults occurred in nursing and residential care facilities alone. In 2012, the BLS Census of Fatal Occupational Injuries (CFOI) recorded a preliminary total of 4,383 fatal work injuries, down from a revised count of 4,693 fatal work injuries in 2011. These numbers clearly suggest that healthcare workers are at high risk of workplace violence, and that healthcare establishments should frame enhanced protection strategies.

OSHA recommendations do not directly address workplace violence, but healthcare businesses would be wise to enact their own workplace violence standards. Hospitals must also make annual workplace violence assessments and institute a workplace violence prevention and response plan. Overall there are five key strategies that hospitals may implement to prevent physical violence.
The strategies are:

- Conducting annual baseline workplace violence assessments
- Mandatory training and workplace violence awareness programs
- Reporting of every incident related to workplace violence
- Categorizing every violent incident as a workplace violence incident
- Linking human resources with security to improve workplace violence prevention.

Organizations need to implement distinctive solutions that convince patients to prefer a healthcare service provider to others offering similar services. The strategies adopted by senior management should be aimed at boosting employee morale, and thereby productivity to enhance the quality of care rendered. The designated authorities need to focus on building a safe and secure environment of care by making the necessary investments to achieve optimum health service outcomes.

Asset Protection

Although the protection of occupants cannot be emphasized more, effective asset management in hospitals and healthcare organizations provides an equally strong argument for a robust security program. Hospitals, by nature, are relatively porous environment housing expensive equipment and hazardous chemicals which lure unauthorized access. In this regard, healthcare institutions should begin by identifying asset categories potentially vulnerable to a loss that would interrupt operations, either for a limited time or permanently. Preparing a list of controls that the hospital should be using, followed by assessing the controls in place and ensuring that employees are using them will help in controlling overall protection. The Joint Commission mandates that control access is in place with effective visitor management solutions to protect patient safety and security and to empower the staff. According to the agency, maintaining a friendly environment is not in line with current recommendations for hospital best practices and may lead to staff feeling unsafe at work.

Organizations must develop capabilities to monitor real time high value life-critical assets throughout the facility. An integrated security program comprising sophisticated asset tracking can meet these ever-intensifying security challenges. Achieving these objectives will aid in avoiding non compliance with various industry regulations, improved efficiency at device tracking and avoiding substantive financial costs spent on equipment replacement.

Hospitals face a variety of economic and regulatory pressures that make effective asset management a key part of their success. It is imperative for healthcare organizations to adopt a comprehensive risk management approach that enables the evaluation of asset threats which go beyond financial loss. An incident of theft involving narcotics, radioactive or other hazardous chemicals imply greater threat than the loss of the medical device that contained the materials. This provides another significant argument for the incorporation of enhanced protection strategies to ensure the safety of critical assets to take performance and possibilities of asset management to a new level.

As if the existing potential threats to occupant safety weren't alarming enough, healthcare institutions are facing a threat that has recently begun to emerge. It involves the information security risks associated with networked medical devices. Security researchers have demonstrated that devices such as pacemakers, defibrillators, and insulin pumps which incorporate wireless capabilities and complex software are vulnerable to all evolving forms of cyber attacks. Healthcare security leaders can implement a range of practices to mitigate the risks.
The strategies include:

- Itemized inventorying and ensuring stricter controls on existing devices
- Creating awareness of networked medical device cyber security threats
- Integrating security into device procurement policies
- Mapping flow of patient data
- Using physical safeguards, disaster recovery and resiliency measures
- Collaborating with device manufacturers.

Clearly, entities desirous of disrupting critical services have time and resources – factors lacking for healthcare senior leaders. Organizations need to rise to the threats and collaborate with information technology and compliance authorities to collectively address the security risks in asset management.

Advanced Operational Efficiency

In a hospital, the improvement in process efficiency begins with identifying the primary stages involved in a patient's visit. For each of these stages the manager analyzes the demand and capacity functions, while the management team works towards achieving a warm environment to support the healing process. It is important that the authorities prioritize the most appropriate countermeasures that comply with regulatory mandates, insulate it from liability, and manages the risk of loss and occupant injury. In each of the stages healthcare security managers should assess the technology they currently employ and should constantly seek to explore additional capabilities in the technology to provide security beyond the physical sphere. Identification of expanded capabilities will help reduce operating and maintenance costs, and support higher quality requirements to improve patient care and satisfaction.

Electronic access control systems are garnering increased attention as they enable authorities to control access to areas and resources or computer-based information system. However, electronic access control systems contain important, confidential, or sensitive information that are accessed by numerous authorized users having varying degrees of system accessibility. Therefore, the electronic access control system should be integrated into the overall security framework as a human resources management tool. Enhancing operational efficiency also involve identifying, assessing and averting risks. Hospital security managers should perform risk assessments to identify threats and proactively implement practices to eliminate the risks.

To perform all the tasks, security managers need to constantly prioritize their duties to solve one task over another. As it is not easy to detect all the potential threats throughout an entire organization, security managers need to ensure a suitable atmosphere for people to feel comfortable to speak up about risk areas or near misses. Achieving these objectives will go a long way in staying compliant and avoiding liabilities.

The Joint Commission values risk assessment as a key security management tool. The risk assessment must include asset valuation, threat analysis and determination of likelihood of threat occurrence, a list of existing and potential vulnerabilities and recommendations for mitigating the risks. TJC requires that assessments consider reports to illustrate employee compliance with security and human resources guidelines. It mandates threat analysis as part of the preventive risk assessment, which details every previous incident to draw valuable lessons for future protection. For ensuring effective security of information, operations, people, or facilities applying robust risk management principles can provide a strong foundation.

Avoiding Liability

There can be no denying that healthcare authorities that anticipate and address issues before they become problems can save on time and enormous money otherwise spent in resolving disputes. This factor along with all the others presented above makes a compelling argument for an all-encompassing security program. However, there is a lone factor that weighs of equal value relative to the combination of all these factors combined together – the potential of legal liabilities. Healthcare organizations are litigation targets and face increasing scrutiny from regulatory authorities to ensure the integrity and security pertaining to patient safety, electronic health records, device management, and endpoints. Hospitals are being evaluated by prospective patients and families not only for the quality of care but also for the level of protection provided.

Further, the hospital institution is always liable for use of defective medical instruments or faulty use of a medical device. Ever-changing federal law also complicates the liability of hospitals by adding exceptions where the patient has reasons to believe that the doctor is employed by the hospital, even if the doctor is an independent contractor rather than an employee. Simply put, hospitals are liable for actions performed by independent contractors on a variety of grounds. Furthermore, asset records inconsistencies render a hospital non compliant under TJC and HIPAA. Establishing a corporate culture of compliance with regulatory requirements will advantage any healthcare center if it becomes a target for litigation.

The law affecting healthcare security is developing rapidly and requires that leadership team understands the scope and trends of litigation affecting liability in hospitals and medical centers, in order to better prepare for compliance and requirements of The Joint Commission, HIPAA, CMS and all other accreditation inspections. This necessitates that hospital security managers understand the causes of security liability, legal concepts associated with negligence and specific actions that can prevent liability in supporting the preventative risk management program of the organization. It is possible to manage liabilities through applying effective and efficient systems that prove to be helpful for the organization from all aspects.

Healthcare service providers are required to bill private health insurers and Medicare as the most common types of third party. However, Medicaid is always the payer of last resort and organizations should bill third parties – long-term care insurance, other federal programs, court judgments or settlements from a liability insurer, etc. – before billing Medicaid.

As a provider of care the responsibility of a hospital begins as soon as it agrees to treat a Medicaid eligible patient. After the individual is accepted as a Medicaid patient, the hospital is obligated to follow Medicaid's third party liability guidelines and other policies, must ensure at every step that the patient is eligible for Medicaid.
The medical center should also perform a Medicaid eligibility check again when entering a claim, as eligibility and Third Party Liability information are constantly updated. These diverse requirements call for a robust security program that will collaborate at each step to maintain all records related to regulatory matters and ultimately help to comply with the necessary regulatory requirements.

Hospitals being most dynamic of public places must remain vigilant throughout while maintaining privacy and the continuity of care. In a scenario of changing regulations, emergency planning, evaluations and unannounced inspections a comprehensive security program serves as an important multifaceted part of your healthcare environment. The security program becomes a preferred compliance and security partner for hospitals and healthcare facilities as they plan, manage and execute their service requirements.