Hospitals Meet Security Challenges with Integrated Security and Facility Solutions

by Steve Nibbelink, CHPA

January 2012 / White paper
# Summary

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>Healthcare security issues today</td>
<td>5</td>
</tr>
<tr>
<td>Security technology throughout the healthcare facility</td>
<td>8</td>
</tr>
<tr>
<td>Access control</td>
<td>8</td>
</tr>
<tr>
<td>Video surveillance</td>
<td>9</td>
</tr>
<tr>
<td>Patient, staff, and asset tracking &amp; management</td>
<td>10</td>
</tr>
<tr>
<td>A day in the life of an intelligent security management solution</td>
<td>11</td>
</tr>
<tr>
<td>Conclusion</td>
<td>14</td>
</tr>
</tbody>
</table>
Executive summary

As healthcare facilities grow larger and provide around-the-clock care, they become increasingly more vulnerable to a wide variety of security threats. And as country-specific healthcare guidelines mandate varying levels of security under its “environment of care” standards, it is left to each hospital and healthcare organisation to decide on the right tools and solutions to meet their security and facility needs.

The first responsibility and mission of any healthcare organisation is to ensure patient safety and quality care. The security and safety team; the recruitment, training, and education of their personnel; their policies and procedures; and their technology tools and solutions are all designed to support the life-saving mission of the healthcare organisation.

For the hospital security and safety team, their goal is to create an identifiable and repeatable process for each of the challenges identified during the risk assessment and gap analysis and in the ongoing security management plan.

These professionals have many tools at their disposal as they create their own programs, policies, and procedures. They examine their own unique physical and community environments; the administrative philosophy regarding security; and the expectation of the patients, visitors, medical/clinical staff, and support staff; as well as industry best practices. Each healthcare organisation has the opportunity to utilise technology, or physical security components, to create a safe and secure environment for everyone and everything on the hospital campus.

These components of physical security include:

- access control
- video surveillance
- infant tagging
- patient management
- intrusion detection
- intercom communications
- panic alarms
- staff management
- asset management/RTLS
- mass notification communications
- visitor management
- parking management
- emergency communications
- smart/financial cards
If each of these technology systems is purchased, administered, and maintained on a separate and individual basis, it causes the hospital to incur undue expenses and operational inefficiencies. However, when they are part of an integrated, technology master plan, the healthcare organisation can improve security and operational efficiencies, while also reducing the associated cost. In fact, in *Hospital and Healthcare Security*¹, the authors state, “Authorities estimate between 3 and 10 percent of hospital expenditures could be saved if proper security controls were implemented.”

This white paper will discuss the growing security issues in hospitals, including violence against hospital staff, patient elopements, and infant abductions. We will then examine three components of an intelligent security management system – access control, video surveillance, and real-time location system tracking for the monitoring of patients, infants, and hospital assets. Finally, using a “day in the life” scenario, situational examples highlight the integration benefits of these technologies in a comprehensive and intelligent security management solution. With real-time actionable data provided through such a solution, security personnel, staff, and hospital executives have the fundamental information at their fingertips to improve hospital security, safety, patient flow, and financial health.

The statistics regarding crime and violence in hospitals is staggering, and clearly indicate that security is a concern for hospitals around the world. For instance, the International Association for Healthcare Security & Safety (IAHSS) 2010 Crime and Security Trends Survey reports four categories of criminal incidents—simple assault, larceny, vandalism, and burglary—accounted for 91 percent of all reported crimes in US hospitals in 2010, nearly doubling since the last survey in 2004.

Additionally, a 2011 study by the Emergency Nurses Association reports that from January 2010 to January 2011, more than half (53.4 percent) of nurses reported experiencing verbal abuse and more than one in ten (12.9 percent) reported experiencing physical violence over a 7-day period. Patients were the perpetrators in nearly all incidents of physical violence (97.8 percent) and verbal abuse (92.3 percent). The study also found that a patient’s room was the most dangerous place for an emergency nurse, with more than four out of five incidents (82 percent) of physical violence occurring in that location.

The National Observatory for Violence in Healthcare (ONVH) in France reported that rising incidences of violence recorded in previous years continued in 2009 with a 38 percent increase in the number of incidents reported. Detailed reporting shows that 45 percent of recorded incidents are categorised as "physical violence" against a person, and most often occur against the caregiver. Finally, 15 percent of reported incidents are crimes against property.

In 2010, The American Society for Industrial Security (ASIS) published a white paper showing that in the United Kingdom and Ireland, a study of 310 accident and emergency departments revealed patients were the most common assailant and nurses the most common victim. In addition, the United Kingdom’s National Health Service (NHS) reports that approximately 25 percent of their medical staff experience personal crime. They also estimate that violence costs their hospitals around 100,000 GBP per year in security, time off for affected staff, and legal costs.

In Australia, one study shows that violence generated from clients, patients, visitors, and relatives accounts for 56 percent of the violence reported in public hospitals and 41 percent of the violence reported in private hospitals.

To address concerns and issues in workplace violence, in June 2010, the Joint Commission published Sentinel Event Alert #45, regarding violence in the healthcare setting, which calls for each healthcare facility to have a documented workplace violence program and process.

---

Yet another challenge is preventing prisoner escape from healthcare facilities. In 2011, the International Healthcare Security & Safety Foundation (IHSSF) commissioned a study that identified the location and percentage of prisoner escapes from four main areas in a hospital:

- Emergency room: 14.1%
- Outside the hospital (e.g., hospital entrance, parking lot, etc): 17.2%
- Clinical treatment: 39.4%
- Restrooms: 29.3%

So, what puts hospitals at risk for crime and security risks? The basic elements and environment of a hospital creates many risks and ongoing challenges including:

**Issues of Risk**
- Healthcare is usually provided 24 hours per day and hospitals are required to be publicly accessible.
- In most locations, healthcare staff are predominately female and are the most likely victims of workplace violence.
- Workplace violence is an increasing problem.
- Drugs are used and stored in the facility.
- Money is handled throughout many healthcare facilities.
- Healthcare facilities can be considered targets for acts of terrorism.

Hospital security is risk-based and incident driven – and as such, hospital security departments are especially challenged to provide a safe and secure environment for their patients, visitors, staff, and assets. When asked about their concerns, hospital security director’s listed the following areas for concern within a hospital:

**Hospital Security Concerns**
- Workplace violence
- Infant/pediatric area(s)
- Emergency room & clinical areas
- Internal/external theft
- Parking lot security
- Staff safety & security
- Pharmacy – central & distributed

**Hospital Organisational Concerns**
- Appropriate staffing levels
- Budget/funding/ROI
- Administration’s apathy about security
- Regulatory compliance
- Officer recruitment, retention, & compensation
- Emergency preparedness
- Patient care changes/roles

**Hospital Technology Concerns**
- Access control & video surveillance
- Patient management solution
- Asset management solution
- Convergence – IT & security
- Integration to other security products
- Integration to non-security solutions
- Computer-aided dispatch/communications

---

Each healthcare organisation has their own set of unique security and safety risks, depending on demographics, service offerings, and administrative strategy. The “security of the healthcare organisation” is a collaborative effort, as the security department is seldom responsible for all the components of the protection program and security management plan (Figure 1).

Figure 1. Collaboration needed for security for healthcare facilities

---

Security technology throughout the healthcare facility

Healthcare facilities use a variety of security technology and solutions that depend on a variety of factors, including:

- physical structures
- services provided
- demographics – patient, workforce, and community
- administrative strategy
- organisational culture
- community culture

Each healthcare security team examines the details of these factors to determine the best mix and use of security technology. We will examine a variety of these technologies and how they might be used in the hospital.

Access control

Access control, or managing access, may be defined as the means by which people are granted or denied access to restricted areas throughout the healthcare facility campus. These areas may include (but are not limited too) the emergency room, maternity area, pediatric area, intensive care units, pharmacy, parking garage/lot and more.

While this definition may be straightforward, early access control systems were as simple as a closed door, a sign, or even an elevator operator. Today, the technology involved and the decisions in design, administration, and use of an access control system can be much more complex, but managing the access to the healthcare facility remains a prime concern for the organisation.

One of the largest security challenges hospitals face is how to secure a space that is intended to be not only a public environment, but also an inviting one. This means that a balance between permissiveness and control is needed, both in the chosen technology, as well as the healthcare facility’s security culture. For example, a hospital may have a sophisticated access control system and card that is also used as the employee’s picture identification, smart card for financial transactions, and staff management/location card.

While sophisticated technology can be a real asset to an organisation – it only takes a “helpful and courteous” employee to defeat the security of the system, by holding open a door for another person. The access control system can be used for the staff, the patients, the visitors, the vendors and the public.

Now, with the patient, the public, and the staff in mind, how does the facility’s management begin to evaluate the many types of access control systems that are available in the market today? Furthermore, in a growing and changing healthcare environment, what is the best kind of access control to meet the current and future needs of security and integration with building, energy, and power solutions?
Video surveillance

In the past, video surveillance systems may have included a Newvicon® or Vidicon® tube camera, sequential, looping or bridging switchers, and video cassette or time lapse recorders for video recording. In addition, security personnel needed to manually change the tapes over the course of the day. Identifying specific events or incidents was both difficult and very time-consuming.

Today, the technology is remarkably different. The cameras today have embedded processors that enable video to be compressed within the device and transmitted over real-time IP networks. Megapixel camera technology has ushered in a new era for the video security industry—providing clear, detailed, and expansive images—while combining sophisticated features such as wide dynamic range; low light, anti-bloom capabilities; and thermal imaging into a single, intelligent camera. The video management software can use new technology as well as extend the life of older camera technology, to better utilise the hospital's current assets and recording solutions. Digital video recorders (DVR) and network video recorders (NVR) can be managed and utilised in both distributed and centralised command and control environments. They have the ability to locate data, process images, and transmit vital information immediately with the ease of graphical user interfaces and interpretive software.

The advent of video analytics brings additional flexibility and increased productivity to the security personnel that monitor and administer the video surveillance system. When an analytic is active, it can send an alarm or warning message or video to remote locations and mobile devices. The analytics software can provide specific and detailed information regarding events and the type of alarm condition—focusing on what is truly important and reducing the amount of false alarms.

The command and control centre can display only the video required for a specific alarm or condition, based on the individual event, the location at the healthcare facility and the security parameters established. Technology can provide the responding security personnel the situational awareness knowledge, so they can more effectively and safely remedy the incident.

The concept of being able to view and record any camera, at any time, from any location is fundamental in optimizing hospital security with video surveillance.
Patient, staff, and asset tracking & management

Whether your patients are in a long-term care facility, behavioral health facility, or a general or acute care hospital, their protection and safety are critically important.

Technology today provides security professionals with the means to incorporate patient management technology into each area (public, restricted, clinical) throughout the healthcare facility and integrate the technology solution into the other components of the healthcare security plan.

Through a variety of RFID and Wi-Fi system solutions, tagging technology, and management software, the patient becomes part of the safe and secure environment. The security personnel and clinical staff can now locate, track, and identify patients throughout the facility, safeguarding against patient wandering, elopement, and abduction.

This solution creates both local and campus wide protection zones, enabling the security team to identify, track, and locate patients, staff, and assets throughout the healthcare campus. As an example, when an alarm condition occurs, real-time video can be displayed at the security command and control centre, to provide surveillance of the alarm location and the individual and/or asset involved in the event. The integration of the access control system can provide strategically managed access points to filter the adverse event to selected areas where security and staff can resolve the issue. The “alarm conditions” can be configured based on:

- type of patient
- areas or zones within the hospital
- each staff member
- for emergency response in workplace violence or security incidents
- for managing and monitoring patient flow and associated choke points
- for managing and monitoring hand hygiene compliance standards
- the use and location of hospital assets, such as medical equipment for patient care
A day in the life of an intelligent security management solution

The process of security integration can be as simple as a video surveillance image associated with an access control door, or it can be as comprehensive as the following scenario.

A nurse enters the healthcare facility’s parking garage by presenting her access control card (which is also her photo identification card) to the access control card reader at the garage entrance. The card is read, accepted, and the barrier gate is raised for entry into the garage. The acceptance of the card also activates her staff management tag, so she is now an active employee in the staff management localisation, tracking, and identification system.

As she moves from the garage into the hospital, she starts her day in the intensive care unit, ready to care for her patients. One of her patients, recovering from an operation, has a patient management tag which identifies the patient and the room the patient occupies. In the room, the medical equipment has asset management tags on each device which associates the equipment to the room and the patient, enabling the nurse access to a complete record of all the equipment needed for the patient’s care. She also has access to the information necessary to identify needed equipment when required, as all of the hospital’s medical equipment and assets are identified and tracked through the asset management system.

This hospital, the caregivers, and the security team have the best possible solution in place to monitor the status and location of the equipment, its current state in terms of maintenance and service requirements, and the life cycle cost management. And when this real-time data is integrated into the security and asset management procedures, it optimises asset use and can reduce the associated costs of buying additional or extra pieces of medical and administrative equipment.

As the nurse enters the patient’s room, she uses the hand hygiene station, where her badge is scanned and her use of the device is recorded in the hand hygiene monitoring compliance software to maintain and monitor compliance, providing documentation for continual process improvement in eliminating hospital acquired infections.

Meanwhile, the pharmacy fulfills a needed prescription for the patient, and the medication is transported to the intensive care unit, and monitored throughout the process by the asset and staff management tags associated with the drug, the transport cart, and the staff member to increase the safety and security of the process.

While this “normal” routine is in progress, the emergency room is actively treating patients with a variety of medical needs. There is however a disturbance in the emergency room treatment area. The severity of the incident requires the hospital to lock down the area through restricted access.
capabilities, which is accomplished through the access control system. The integration of staff and asset management solutions with the access control and video surveillance solutions provide the hospital with a complete roster of patients, employees, and medical equipment (hospital assets) in the secured area, as well as surveillance of the area to supplement the security response.

Throughout the hospital, the integrated solutions also provide data on the status of patient flow to better manage the medical care of the patients by understanding where the patients are in the process of the treatments, where there is a bottleneck, and to make sure the appropriate number of healthcare providers are available where and when needed.

Additionally, the facilities management team gathers data from the temperature sensing device in key entry/exit locations, compares the temperature data to the access control records for door openings/closings, and can then work with the security team to adjust door opening times to minimize temperature variations in the physical space.

At the same time, the security and access control technology accumulates, manages, and presents incident data so trending information can be analyzed as to the most frequent events, individuals involved, locations of security incidents and the security response and disposition of the incident. Having all security information available through a comprehensive dashboard further improves the availability of actionable information and corresponding response times (Figure 2).

As the security team plans for the best use of their security officers, they use the discussed technology, not only as their “force multiplier,” but also to ensure they have the right number of security officers available, at the right place, at the right time.
The careful planning, implementation, and integration of these multiple technologies, as well as the development of policies, procedures, and programs, including training and education, allows the hospital to continue operations in a safer and more secure environment throughout the healthcare facility.

For the security team, the primary benefit of an integrated security and building management solution is the optimised support and contribution to the life saving mission of the healthcare facility.
Conclusion

On a daily basis, the patients, visitors, staff, and community enter and interact with their local hospital and healthcare providers – most of the time unaware of the security and safety professionals and technology needed to provide a welcoming, safe, and secure environment. Providing such an environment is a collaborative effort between the security and safety team and all the other departments in the hospital, and is a basic requirement and expectation for every healthcare organisation.

Intelligent security management solutions, such as patient and staff management, asset management, access control, video surveillance support the security team’s mission with real-time actionable information that enables them to detect anomalies and respond more quickly to potential threats before they become incidents. Furthermore, by aggregating all hospital security data onto one user-friendly dashboard, security personnel can easily monitor their entire hospital campus. And if there is an incident, this data provides hospitals with a full, automatic audit trail.

In addition, by using a common IP-based IT infrastructure, integration of security solutions with facility and building management systems leads to an increasingly intelligent, efficient, and cost-effective healthcare facility. Furthermore, this same open protocol enables hospitals to leverage their existing security investments, while also taking advantage of newer and more advanced technologies to create a comprehensive security approach.

With an intelligent security management solution in place, hospital executives can rest assured that their facility is well equipped with the fundamental tools needed to support the life-saving mission of their healthcare organisation.