Healthcare: Layering Security & Internal Access Control

ASSA ABLOY

The global leader in door opening solutions

Protecting Your Greatest Assets

Picture the following… a newborn being transported from Labor and Delivery (L&D); a family coming in the hospital front entrance to visit their elderly father; a rear exterior door to the hospital propped open so staff can take a break; a hospital employee noticing certain supplies diminishing on a regular basis; an influx of visitors during the shift change on the behavioral health unit… and an anticipated increase in patients through the Emergency Department (ED) due to a virus of epidemic proportions. Now picture the satellite functions and procedures performed by that same hospital system at remote ambulatory care facilities and medical office buildings. Each of these provides a view into the Environment of Care (EOC).

Where are the eyes and ears to ensure the safety of that newborn? Does that family have any confidence that their smart phones, tablets and other personal devices will be safe if they go to get their father a snack? How often is that rear entrance open and does anyone know who might be accessing the hospital through that door? How does the hospital system protect clinical, professional, administrative and environmental staff from suspicion of diverting supplies? What are the visitor tracking and patient protection procedures to ensure safety for everyone — even in the case of a possible epidemic or weather-related crisis? And what access control system ties those satellite facilities to the main hospital?

Consideration of these and many more facets of hospital life provoke a host of thoughts about security, convenience, patient, visitor and staff safety, even energy efficiency and resilience in the face of disasters. These are weighty topics that require input from virtually every department in the hospital because they form the Environment of Care (EOC). The EOC is comprised of three basic elements: building and space, equipment and people.

The first step in planning for security in this complex environment is to identify the stakeholders and decision makers who have a lot invested in the outcomes – whether related to compliance, the delivery of care or the successful protection of people and assets.

Stakeholders in the Healthcare Environment

A Reconfigured Team

Major departments in the hospital are now collectively involved in decisions that affect the delivery of healthcare: patient safety, HCAHPS scores, building design, access control, employee training, and more. No longer are decisions made in the vacuum of one's own department or even within the confines of a single hospital. Consolidation and acquisition in healthcare, as well as the requirements for reimbursement from the Centers for Medicare and Medicaid Services (CMS) have changed the game. Healthcare administrators, operations personnel, in fact every department, has recognized that decisions made in one area of the hospital system may affect every other area. This can be called the domino effect that can make or break a hospital's reputation.

Every hospital wants its reputation to get the highest marks for welcoming families, caring for patients, retaining staff, and securing supplies, medical equipment and controlled substances. As hospitals adjust to the changes associated with the Affordable Care Act and cope with other changes in the delivery of care, consensus building and collaboration become the basis on which decisions are made. So who is at the table?

Resilience Officer

This is where responsibility rests for maintaining the systems required to offer healthcare in the case of a disaster to the magnitude of Hurricane Sandy which took place in October 2012 in the Northeast. From infrastructure to security to staffing, this position touches every other department in the hospital. Concerns about security are uppermost as the hospital facility will be the first point of entry for those affected by storm, casualty, even acts of aggression. Hospitals today have made the commitment to stand strong and ready when virtually every other building is in rubble. The scope of this position secures the exterior, identifies authorized personnel, prepares for infection control, and ensures that infrastructure and life-safety equipment as well as life-saving medicines are secured and ready.

Patient Experience Officer

Often referred to as the "CXO" or the Chief Experience Officer, this professional looks holistically at the hospital's methods from Admitting to X-Ray — to constantly improve the patient experience which translates directly to improved HCAHPS scores — and is the basis for reimbursements from The Center for Medicare and Medicaid Services (CMS). Staff training, staff responsiveness, communication — even in the face of a disaster — are all part of this position's responsibility.

Human Resources

The work of human resources doesn't stop with recruiting, credentialing and on boarding. Once employees are part of the system, training in the vast range of complex systems and procedures that clinical and professional staffs are required to understand, support and perform becomes the major focus of this integral department. Cascading one system across the entire hospital or entire system of facilities translates to improved training outcomes and better implementation. Providing proper protection through creative access control systems can go a long way toward retaining clinical and professional staff… another important factor in HCAHPS and The Joint Commission compliance.

Security

This department is the heartbeat of the hospital with regard to protecting the systems that provide for the hospital.

Operations

Both Administration and Clinical Operations have significant investment in decisions. Pharmacy, Emergency, Infection Control and all other departments are represented within this function. Focusing on Pharmacy as an example, access to and the delivery of Schedule I, II, III, IV and V controlled substances using the "5 rights", is critical. Add to that the need to reduce operating expenses and reduce the incidence of "diverting" supplies, such as linens, scrubs, sterile tubing and saline syringes.

Planning, Design and Construction

It may not appear that this function has a major role. Yet the built environment is a critical element in the delivery of healthcare. Improved patient outcomes and HCAHPS scores can be a function of an enlightened aesthetic. Therefore, interior design, elegant finishes and innovative functionality play a leading role in healthcare today.

Compliance Department

The focus of this department spans the many agencies that ensure compliance with life safety regulations such as NFPA (National Fire Protection Agency) and other authorities having jurisdiction (AHJs). Other critical guidelines and compliance elements include the Americans with Disabilities Act (Yes, ADA is a law) and HIPAA (Health Insurance Portability and Accountability Act…also a law!). The Facility Guidelines Institute (FGI) is another resource for compliance.

Since a great percentage of hospitals' revenue comes from CMS — Centers for Medicare and Medicaid Services — compliance with The Joint Commission, DNV, HFAP or other "deeming" bodies is a high priority.

Layering Security

Multidisciplinary committee decision making, involving representatives from many departments, regarding layering security is the new normal in healthcare. Such decisions are put through a five-lens filter measuring the impact on patients, families, staff, physicians and cost. The Joint Commission requires that all hospitals which they survey develop and implement a performance improvement framework for their processes affecting the safety of patients and everyone else who enters the hospital, the security of everyone who has access to the hospital, fire safety and emergency operations, among others. (The Joint Commission EC01.01.01)

Each hospital would do well to perform an annual risk assessment to point out the need for a security plan for the entire hospital facility or system. This security plan is a major factor in compliance as well as improving the patient experience.

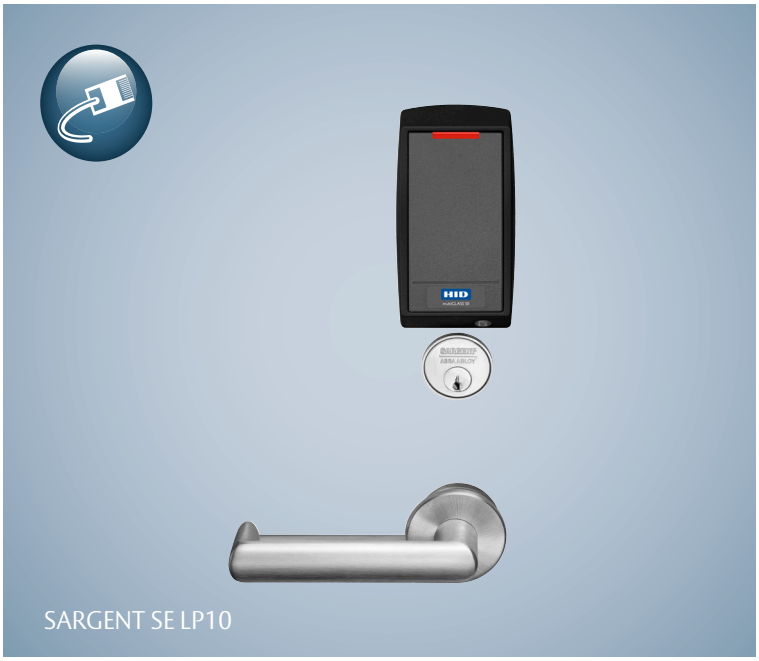
All of this information forms the basis of the "Who, What, When and Where" of a security system, which is an exercise in layering security vertically and scaling that security plan horizontally.

Layering Security? Yes, layering vertically… and scaling the right solutions horizontally. Now that the stakeholders and decision makers have been identified, the hospital can creatively scale security solutions to match the risk associated with each opening. Scaling the security solutions according to risk allows the hospital to maximize the security plan while staying within a budget. High security areas may require more sophisticated, possible online solutions. Lower risk areas may require simpler, off line products. The hospital has far more flexibility in designing a security system in this manner.

Security System Design

Now for the specifics of creative security system design:

1. Define users (clinical staff, general public/visitors, patients, those with disabilities, other populations within the hospital)
2. Identify estimated budget
3. Determine areas of greatest concern (Nursery, ICU, medication stations, Pharmacy, supply cabinets, exterior visitor entrances, employee entrances, linen storage, nurse servers, patient rooms, staff lockers, stairwells, etc)
4. Assign the frequency of use (high traffic or low use areas)
5. Document locations in the building that are subject to fire/egress codes such as NFPA, ICC, IBC, AHJs, and others. In many cases, the hospital has employed "pin code" type devices which do not provide audit trail. Often the codes to access the doors on which this type of device is applied, are either written on the door frame or on a "sticky" note near the opening. This does not follow compliance guidelines. Therefore these locations would be suitable for re-evaluation.
6. Assign a level of security (general access, high security, lockdown areas)
7. Add energy efficiency and/or LEED/Sustainability requirements (doors contribute to significant energy loss from the building envelope)
8. Build in infection control with optional antomicrobial coatings



SARGENT SE LP10

SARGENT HARMONY SERIES

SARGENT Profile Series v.G1.5

MEDECO³ XT and Logic

SARGENT IN120

HES KS00

Scalable Security Solutions

Once these factors have been identified and agreed upon by the committee, selection of devices and the platforms they require can begin. There are many options, some of which are outlined here:

Online Access Control

In the recent past, the only option for online access control was to hard wire every opening. Hard wiring is desirable and even necessary where immediate lockdown or egress might be required, in the case of stairwells, for instance. However, the expense of hard wiring, particularly in the case of a retrofit application can be cost-prohibitive. Adding in the cost of qualified, licensed electricians and other professionals can raise the actual installed costs much higher than expected. There are other ways to accomplish online access control employing two similar platforms.

Wi-Fi

Hospitals today are equipped with a Wi-Fi network that can be employed as the network platform for access control. The main advantage of using Wi-Fi is that it is a perfect solution for non-critical openings that still require monitoring, audit trail and secured access. Wireless devices provide a secure encryption for access codes and, in many cases, can use the existing badge or credential currently employed by the hospital. Another advantage of a Wi-Fi device is that access decisions are authorized "locally", meaning that the locking device does not have to "check-in" with the access control panel. And a record of transactions is maintained in the device at the door.

Wireless

Yes, wireless is different from Wi-Fi. Typically, a wireless device requires a hub or interface that is actually hard-wired back to an access control panel. The advantages of some wireless devices include the following: the card reader or integrated card reader and locking device can be applied directly to the door, making for an aesthetic and cost effective application; these devices often allow application on an historical building, stone, extra thick walls, etc. Because the hub or interface is above the ceiling, the installation of the device on the door is faster and causes far less disruption for the hospital. The programming of these devices is typically done right at the access control system and access can be provided to any and all persons at the time of on-boarding.

Power-Over-Ethernet (PoE)

This platform uses the network power provided by the Cat 5 or Cat 6 cable that is installed throughout the hospital. The main advantage of PoE is the significantly reduced energy cost. Devices on PoE act just like hard-wired devices and provide immediate tracking on the access control system.

Offline Devices

There are many openings in the hospital that do not require high security. Offline access control often suffices to prevent unauthorized access without connecting to a large head-end system. Such areas can be secured with pin pad only devices that do not provide audit trail or monitoring.

Electronic Cylinders

Yes, there is such a thing. Often referred to a "portable security" some electronic cylinders can replace existing mortise cylinders and provide simple access control. These devices use a battery powered key to program the cylinder locally. It can also be web-based. Another advantage is that electronic cylinders are available in a number of form factors that allow application to remote or fenced areas of the hospital campus, such as large equipment storage where padlocks might be used. Other areas might include a cash office or the cabinets on trucks or other areas.

The object of this exercise is to "scale" the security solution to fit the unique needs of the hospital or system. Most of the platform solutions can be cascaded across an entire healthcare system, even one with locations in different states.

Beyond Security

Other aspects of facility operations can also be addressed simultaneously with security:

Aesthetics

In the drive to improve patient outcomes, today's healthcare facilities feature pleasing designs that create a relaxing atmosphere. Decorative doors and hardware deliver security without sacrificing design.

Resilience

Geography determines whether specialized door openings are needed to protect against hurricanes and tornadoes. Door opening assemblies tested to withstand destructive storms will help a healthcare organization continue normal operations once the danger has passed.

Sustainability

Hardwired locks that draw low power consumption and insulated doorways that block heat transfer and air leakage improve the energy efficiency of a facility and help meet sustainability goals. Transparency statements tied to these products will verify their contents and ensure they are free of harmful chemicals. Hospitals would be wise to partner with suppliers that issue EPD (Environmental Product Declaration) and HPD (Health Product Declaration) documents with full transparency.

Sound Attenuation

Peace and quiet are hallmarks of a restorative environment. Sound Transmission Class (STC) rated doorways on patient rooms block out the noises that accompany the hustle and bustle of a hospital hallway.

Loss Prevention

Pharmaceutical distribution, storage cabinets, employee lockers — even server cabinets and their sensitive data — are prone to theft. These small doorways, typically on cabinets, can be protected with a new generation of cabinet locks that connect wirelessly with the building security control system. The locks communicate with a nearby hub that relays signals back and forth with the head-end system. So these often overlooked doorways, even if found on a portable cart, are now incorporated as another layer of security that can be monitored and tracked.

With the wide range of locking technologies now available, it's easier than ever to tailor the access control capabilities of each opening to match exact security needs. Hospitals can implement varying degrees of access control at each opening whether it's a loading dock on the building perimeter or a cabinet door in a patient room and everything in between. The locking technologies employed at each opening mesh together and operate seamlessly with the building control system to create a fully secure facility.

Successfully layering security in this manner requires input from all stakeholders to identify risks, applicable codes and regulations that need to be met, sustainability goals, aesthetic preferences and budgetary concerns. When the needs of each stakeholder are mapped out vertically, security solutions can then be layered horizontally to achieve the desired goals and deliver the best possible outcome.