NOVEMBER/DECEMBER 2022

BEST PRACTICES:
HEALTHCARE SECURITY

WHAT'S INSIDE:

To borrow from Jay-Z: Hospital security directors have 99 problems, and access control is involved in nearly every single one. **Page 2**

Partnered ads inside this issue:

Photo illustrations by iStock

UNRAELLING THE COMPLEXITIES OF HEALTHCARE ACCESS CONTROL

To borrow from Jay-Z: Hospital security directors have 99 problems, and access control is involved in nearly every single one.

Just a quick, highly abridged list of things a hospital access control system must account for: critical emergency access that is open to the public, securing potent narcotics, hazardous waste, some of the most sensitive and punitive privacy regulations in existence, quarantine areas, and that doesn't even touch the challenge of keeping track of patients, friends and family of patients, and caregivers who are often in chaotic or intense emotional conditions.

Security Management called on two members of the ASIS Healthcare Security Community Steering Committee to discuss the latest in hospital access management.

William Marcisz, CPP, president and chief consultant for Strategic Security Management Consulting, was in law enforcement before transitioning into private security at a hospital. He has 40 years of healthcare experience—32 years in security administration and consulting, and eight years practicing law. Dan Yaross, CPP, is the director, protective services, at a pediatric hospital in Ohio. Yaross retired from the U.S. Army Military Police in 1995 and launched a 20-plus year career in pediatric health facility security.

The questions and answers below have been edited for length and clarity.

SM: Controlling access in a hospital would seem to be incredibly complex with all of the different layers of protection needed and constituencies that need to be accounted for. Yet the more complex an access control system is, the harder it is to monitor and the harder it is for employees to respect and follow those procedures. How can hospitals reconcile these two aspects?

Marcisz: It's quite challenging. Certainly, you run into a lot of folks, department heads, or administrators who feel that hospital access control should resemble something you'd see in the Pentagon. If you have a very large hospital with 5,000 employees in it, many of those employees need access to the

Danger approaches fast. Be faster.

MAIN ENTRY LOCKDOWN

Our solution keeps outside threats out with a click of a button, mouse, fob or key switch. Instant lockdown at a fraction of the cost of all-motorized latch retraction—that's the Detex effect.

Call 800-729-3839 detex.com/lockdown29

DETEX®

departments that those administrators would like to see locked down—folks like food service tray passers, phlebotomists going up to draw blood, environmental services folks, they all need access to areas. For individual departments that want a high level of access control, the system can and will keep people out. However, to ensure the desired level of service and continuity of care is administered, the department should have a dedicated person to serve as the gatekeeper for employees and visitors who have been excluded from the list of team members who require access.

I try to counsel clients to think about it like this: you've hired employees, you have to have a certain level of trust. I think having more of an open access for employees is a good idea, while limiting the number of areas with tight access control to areas that absolutely need it.

Yaross: In our case, as a pediatric facility, we were granted a variance from the fire code so we are able to secure both sides of in-patient units. The auditing department thought almost all of our hospital should be treated as security-sensitive and tightly controlled. But looking at who needs access, as Bill said, from foodservice to pharmacy to people bringing supplies, there's a lot of people that have access needs.

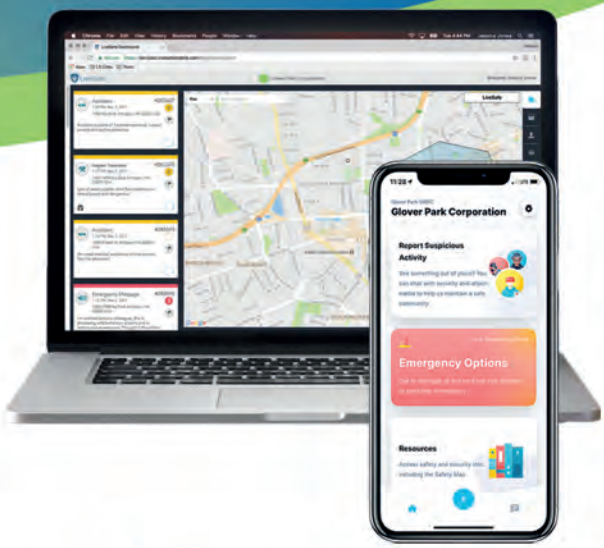
We labeled four security-sensitive areas with our security management plan based on the joint commission requirements and IAHSS [International Association for Healthcare Security and Safety] guidelines. For those we have very restrictive access control. We audit those names with the head of those departments, including pharmacy, NICU [neonatal intensive care unit], emergency, and behavior health, just to ensure that the staff who are granted access truly need it.

SM: The pandemic caused most hospitals to severely limit or even eliminate visitors to prevent the spread of COVID-19. Now that we're on the other side of the severe restrictions, how have you seen hospital access control change?

CONTINUED ON PAGE 6

The Top Solutions for Security, Risk Management and Safety Professionals

Empower and Protect your Organization with the Leading Platforms for Risk and EHS Management and Safety Communications for Everyday or Urgent Scenarios



Vector LiveSafe™

Identify safety and security threats, send emergency notifications, and engage employees with two-way safety communications.

Vector EHS Management™

Conduct risk assessments, identify controls, and remediate hazards.

VectorSolutions.com/RiskManagement

VectorSolutions™

Marcisz: During the last couple of years, hospitals secured their perimeters and only allow access through one or two, or sometimes three, doors, all of which have screening points. To make hospital operations flow smoother and make it easier for patients and visitors to come into facilities, some hospitals moved service points closer to those entrances. Some hospitals took advantage of the new entry design and implemented 24/7 visitor management.

There's always a tension between convenience and security. Throwing open those doors and returning to the hospital's prepandemic, open-perimeter access design may not be a good idea. Many have discovered there is no need to do so and the new perimeter and screening designs create a safer environment.

SM: Do you have an example of an access control change that a hospital made as a result of that convenience factor or because a security gap was identified?

Yaross: We are constantly looking at this issue. Being a children's hospital, we have a significantly larger scope of restrictions for visitors. We implemented a visitor management system years ago. However, I noticed when I got up here that we weren't doing what I thought was the right thing to do, which is vetting all visitors to the inpatient units on campus. We have many parents or guardians who cannot stay overnight with their kids, and the kids are left alone. Nursing, especially nowadays, is sometimes critically low. They don't have the time to watch every patient room to ensure unauthorized visitors do not enter.

One step we took as a result is that every visitor to the inpatient side is checked against the Federal Sex Offender Registry. I got pushback from a number of departments, saying it was too intrusive, that it wasn't family-centered care, and we shouldn't be asking or getting involved in checking out the backgrounds of patients' visitors.

SM: What do you do when a parent or guardian comes back positive on the registry screening? You don't bar them from seeing their kid?

Yaross: No, we don't. First, only 24 percent of the registry matches we get are confirmed. Seventy-six percent are false matches for a variety of reasons: names are close or there's a data entry error. When there's a match, the information desk calls one of our protective service officers. We have a discrete conversation with the individual, and most mix-ups are cleared up then. And if it's truly a confirmed sexual offender who is a parent or guardian, we will create a safety plan the nursing unit and social work. If it's a Tier II or III offender, that plan will include an officer escort for the individual.

Sometimes it takes some careful explanation to show why a security measure is important. In this case, I asked, "Let's say your child was here alone overnight because you needed to go home to care for another child. Would you feel better knowing that we were screening against the registry so we know the offender status of other visitors in the hospital?"

SM: What are ways to ensure that your access control systems are working properly and that staff follow your processes and procedures?

Marcisz: There are different types of auding you can do. Most access control systems are pretty sophisticated, and you can see who is going through card and multifactor access doors in real time if you really want to track that in a finite level. I think what Dan was saying earlier is just go through card-group access lists with department heads periodically. It doesn't have to be every month, but you should do it periodically, and determine who needs to be in that department or building.

Also, consider the design of your card groups. One tendency is to start from a perspective that is the most restrictive, where you identify the people you think need access and grant only them access. When you do this in a hospital, you end up being too restrictive—you're going to find out quickly that there are many more folks needing regular access to a space than you think. I advise the opposite. When looking at an area, decide who needs to be restricted, know why you are restricting them, and then restrict access. This approach will cut down the number of times you have to go back and reprogram your card groups.

Yaross: We'll get alerts. It's all about collaboration because we keep stressing to our employee population that we only have so many protective services officers. We need all your eyes and ears to alert us quickly. Don't be afraid that you're going to be embarrassed or that you're bothering us. If there's an issue with door readers or you think people are getting in your space that shouldn't be there, we get alerted. Many times, we find out there is an issue with a card reader or the door mechanism might not be functioning properly. We find out a lot about access control issues just through our employees being alert and letting us know when things do not seem right.

Wear it.

To ensure quality of care.

Axis wearable video solutions make healthcare professionals, patients, and residents feel safer and behave better. They deter aggression and abuse before it happens. And they provide an indisputable record that can help you resolve conflicts. They're also easy-to-use, cost-effective, and they work with your existing monitoring system*. Plus, they're backed by our worldwide support network.

So just plug them in. Clip them on. And keep your people safe and sound.

Visit www.axis.com/bodyworn/industries to learn more.

*Thanks to open architecture, Axis body worn camera systems can be used with third-party VMS Video Management System (VMS) and Evidence Management System (EMS), on-premise or in the cloud, or delivered as an end-to-end solution using AXIS Camera Station VMS and AXIS Case Insight EMS.

AXIS COMMUNICATIONS

Let Us Help You Secure the School Better

We've Been Creating Proven School Security Technology Solutions for Decades

CLASSROOM LOCKS & LOCK-DOWN

DOOR-PROPPING ALARMS & MONITORING

SECURITY & FIRE ALARMS & REPORTING

WIRELESS NETWORKED ACCESS CONTROL

EMBEDDED & ENTERPRISE SYSTEMS W/ VISITOR MGT

ACTIVE SHOOTER DETECTION VIDEO & AUDIO

See us at ISC East, NAPCO Booth 903

Contact Us: Together, We Can Take the Next Best-Steps for the Safety of Students & Staff

NAPCO SECURITY TECHNOLOGIES

1.800.645.9445 | salesinfo@napcosecurity.com

www.savischool.com