SIW SECURITY INFOWATCH.COM

HEALTHCARE SECURITY IS A CHALLENGE FOR ADMINISTRATORS AND STAFF

BOTH PHYSICAL AND CYBER SECURITY THREATS POSE RISKS TO PATIENTS AND HOSPITAL STAFF

Sponsored by:

evolv

TABLE OF CONTENTS

AD INDEX

evolv

Visit **www.evolvtechnology.com**

Experience Evolv's Advanced Security Technology

Seeing is Believing.

Evolv Technology (NASDAQ: EVLV) is designed to transform human security to make a safer, faster, and better experience for the world's most iconic venues and companies as well as schools, hospitals, and public spaces, using industry leading artificial intelligence (AI)-powered screening and analytics.

Evolv's mission is to transform security to create a safer world to live, work, learn, and play - providing a connected and layered approach that integrates people and technology to help deter, detect, and orchestrate response to physical security threats.

Prevent and Detect

Technology: A layered approach to help enhance security, situational awareness, and threat response.

Advance Operations

Process: From fit to deployment and ongoing ConOps, our security experts partner with you.

Empower Staff

People: From crowd flow to alert resolution and red teaming, our security experts are there to train.

The Future of Access Control Solutions in Healthcare

Four perspectives spotlight an industry that strives toward integrated, interoperable and secure access control solutions

Lee Odess

In the complex world of healthcare, as organizations continue to expand and evolve, the need for robust and interoperable systems is becoming increasingly critical. This article, created by three member organizations of the Access Control Executive Brief, brings together three insightful perspectives that delve into the challenges and opportunities within healthcare security, specifically focusing on access control systems.

We first hear from Ryan Schonfeld, Founder & CEO of HiveWatch, discussing the changing nature of healthcare institutions and the complexity of incorporating new technologies within their security systems. The second piece by TDSi explores how modernizing access control systems can beneficially impact the healthcare sector by ensuring security and safety while facilitating efficient operations. Lastly, 4S Security presents a compelling case for digital integration in access control systems, emphasizing the pivotal role of system integrators in the healthcare security landscape.

Are you ready to take the next step in enhancing your healthcare organization's access control system and operability? A suitable place to start is below. When asked to put together our thoughts on innovation in access control, specifically in the healthcare vertical, I knew precisely which three members of the Access Control Executive Brief we needed to hear from. I wanted a global view from three different areas of the industry and those with one leg in the old but an even bigger leg leading the new.

THE IMPORTANCE OF INTEROPERABILITY AND CENTRALIZATION IN HEALTHCARE SECURITY SYSTEMS

By Ryan Schonfeld, Founder & CEO, HiveWatch

The changing nature of the healthcare industry is the main reason issues related to interoperability are so critical. Healthcare organizations are constantly growing and changing, adding remote facilities, building in new areas, and incorporating practices into the facility's footprint. This can be a recipe for disaster if physical security teams are not able to seamlessly integrate new – and many times, different – technologies together. Particularly in healthcare, organizations are growing exponentially through mergers and acquisitions, which also significantly increases the complexities around modernizing an access control program.

The healthcare campus ecosystem may contain hospitals, retail/community clinics, research labs and education buildings. It requires flexibility and solutions that can be catered to the specific operating environment while also allowing for interoperability.

Historically, the access control industry has leaned heavily on proprietary technologies requiring extensive integration work to incorporate basic functionality with video surveillance technology and management. Not only does this create a heavy lift for security leaders to incorporate new locations into a security ecosystem, but it can also have a detrimental effect on the oversight of remote locations within the same network of systems. Without the ability to integrate multiple physical access control solutions to create a common operational picture, GSOC operators may be tasked with jumping from platform to platform to address incidents, clear (or respond to) alarms, or shift resources where they're needed most.

When you use multiple platforms without a place to centralize, you end up spreading key data into different systems. Given the rigor with which healthcare data is managed, the result is that now you have more systems that you must ensure are compliant, meaning that the regulatory bandwidth of the organization may be crunched. Healthcare security teams are limiting themselves from operational excellence when using multiple systems because they can't begin to start making data-driven decisions when having to jump between multiple pools of data. The task of cleaning data to glean insights becomes cumbersome for security teams that are already tasked with some of the highest priorities in ensuring the safety and security of patients, visitors, and staff.

Data from not only access control solutions, but also video surveillance data, can become more of a tool for better decision-making when funneled through a centralized security operations management platform which performs normalization of data across disparate input systems. A singular platform is quicker to learn and easier for security leaders to train on, instead of what can be dozens of platforms for each access control solution in place across a healthcare campus.

Data is another reason access control interoperability is critical within the healthcare environment. Too often, we leave data on the table because we don't know how to use it properly. We aren't sure where it lives, where to view it, how to access it in real time, or how to normalize it. And you can't realize its full potential until you do. Access control data is one of the biggest pools of data we have in security – and coupled with information coming in from video, building management systems, intelligence platforms, social media, intrusion alarms, and perimeter security solutions, it has the potential to revolutionize how security teams respond to and proactively address incidents. Some of this data can be applied to the use of field resources and guards, ensuring these costly resources are adequately distributed across healthcare facilities.

Healthcare security leaders must have data to make better decisions, and without significant steps toward bringing disparate systems together, the prioritization of interoperability of access control solutions, or stepping away from leaving critical data "on the table," it's a long road ahead to secure these organizations. Centralized security operations management can mean all the difference.

"There are always distinctive challenges when addressing the specific access control requirements for any business sector and healthcare is certainly no different."

HOW IS THE PUSH TO MODERNIZE ACCESS CONTROL SYSTEMS AND THEIR INTEROPERABILITY HELPING THE HEALTHCARE VERTICAL?

By TDSi

Secure access control is essential for the Healthcare sector in protecting patients and medical staff, along with other inextricably linked assets such as facilities, equipment, medicines and supplies. The unique requirements of each healthcare facility mean medical service providers must invest in the right level of access control to ensure security and safety, whilst enabling staff and patients to easily reach where they need to be.

There are always distinctive challenges when addressing the specific access control requirements for any business sector and healthcare is certainly no different. For example, with the need for both security and infection control, traditional keycards may not always be suitable for all medical facilities. Whilst mobile device credentials have become a popular choice for many secure access control applications, their use within medical facilities may be restricted by privacy and cleanliness requirements, and therefore integration and use of modern contactless biometric readers (such as facial recognition) may be more suitable.

The close integration of access control with other security and IT systems provides many other highly valued features that may benefit healthcare providers. TDSi's GARDiS Access Control solution for instance integrates with Suprema's Biometric Readers for fast and secure biometric authentication and with CCTV and VMS providers such as Pelco, Hanwha Vision and Milestone to incorporate CCTV surveillance data from across a facility and its surrounding site.

Other integrations such as Microsoft's Active Directory can be combined within GARDiS Software to give security and management teams a detailed overview of the security and broader management of people and property across the whole facility, enabling a coordinated response to any potential issues or threats.

As the 'eyes and ears' of the secured facility, these fully integrated systems are also well placed to help fulfill facilities management requirements. Systems such as these can be configured to trigger and dismiss heating, ventilation, and lighting in communal areas to maximize efficiency and minimize the wastage of resources. Secure access control can equally be used for time and attendance monitoring (accurately checking staff arrivals and departures) and integrate with workflows to assist with compliance records and help with staff rotes, especially when CCTV data can also be incorporated should evidence be required.

Fully integrated access control and security systems can help to protect patient privacy and aid with regulatory compliance. They help to manage safe and secure visitor access (by tracking and verifying visitors whilst securing sensitive areas), protect assets, and promote safety during emergencies by notifying people during evacuation for quick and coordinated responses (such as locking down certain areas or providing access to emergency response teams).

This advanced access control as a service delivery model provides exactly the

resources required for scalability and can help avoid some of the high CapEx costs associated with buying and installing a system directly. By delivering an attractive blend of reliable security automation and safety, along with sensible operating costs, Healthcare providers investing in current access control systems have the peace of mind that these critical facilities are properly protected. This enables a greater focus of resources on the primary purpose of healthcare facilities - caregiving and providing patients with the best service and support available.

"In healthcare, where security is paramount, this interoperability is not just a convenience; it's a necessity."

NAVIGATING THE FUTURE OF HEALTHCARE SECURITY AND THE ROLE OF DIGITAL INTEGRATION IN ACCESS CONTROL SYSTEMS

by 4S Security

In the rapidly evolving landscape of healthcare security, the concept of interoperability has emerged as a cornerstone in the pursuit of digital transformation. FHIR APIs and other forms of interoperability between scheduling, care, customer service, and other areas of healthcare organizations are rapidly shifting to modern applications that create a web of interconnected systems, allowing data to transfer seamlessly from hospital to hospital.

However, in the quest for compatibility, one key area of hospitals has been overlooked – the buildings themselves. As hospitals seek to provide an integrated and safe experience even further for patients and staff alike, the key may lie in utilizing the data and physical systems in their building as a part of their goals. Interoperability, in the context of access control systems, refers to the ability of diverse systems and software applications to communicate, exchange data and utilize the information that has been exchanged effectively.

In healthcare, where security is paramount, this interoperability is not just a convenience; it's a necessity. Consider these two examples. A hospital is notified that a case of COVID-19 or another highly infectious disease has been found in their facility. By using contact tracing technology and tying access control data to it, the software can quickly analyze exactly where a patient has been, and whom they've interacted with, and staff can quickly initiate and emergency lockdown.

In the second example, a hospital providing controversial medical services such as gender conversions or abortions receives an online booking appointment through their website. The patient arrives, is checked

in by a front desk agent, and is brought to an exam room. When the nurse enters his room, he violently attacks her. It is found later in the investigation that this man has a history of hate crimes against LGBTQ organizations. To combat situations like these, they need to be stopped before they begin. By implementing visitor management systems and integra8ng them with local watchlists of hate crime offenders as well as integrating with the hospital's EHR (Electronic Health Records) system, a quick, technical verification, can be made to ascertain whether this booking was created by a bad actor, or a patient in need.

Traditionally, the security integrator's role in healthcare has been to install the selected access control, surveillance, or other systems without considering how they may interact with the hospital's broader array of tools that can guarantee safety and security. We believe that integrators are the key to deeply understanding each organization's needs and creating custom integrations tailored to their specific environments. Product manufacturers have limited bandwidth to customize their products and engineer them for specific clients.

However, by providing integrators tools (Open APIs, Platform Development Tools, etc.) integrators become the conduit that bridges the gaps between functionalities of individual systems and insert them congruously within the broader scope of the organization's application stack and more importantly, safety strategy. Integrators can help connect (integrate), secure (cybersecurity), and maintain (service and support) systems on a personal level to ensure that each organization benefits from tailored solutions rather than blanket offerings from product manufacturers.

Looking ahead, the value of interoperability and the role of the integrator in healthcare will only grow in importance. As technologies such as artificial intelligence, machine learning, and the Internet of Things (IoT) become more prevalent in access control systems, the complexity of integration will increase. The integrator should be at the forefront of this evolution, ensuring that these advanced technologies are successfully incorporated into the healthcare security infrastructure. To fully take advantage of the acceleration of technology in the healthcare space, providers must partner with the right integra8on partners that can help them identify, orchestrate, and implement the technologies that will improve patient care, and staff safety, and ultimately continue to protect their staff, their facilities, and uphold their mission to protect that which we all deeply value – life itself.

IN CONCLUSION

In conclusion, the modernization and integration of access control systems

within healthcare are not just about enhancing security; they are transforming how healthcare organizations operate by making data more accessible, insights more actionable, and decision-making more strategic. As patient safety and data security continue to be paramount, the future of healthcare lies in the hands of those who can effectively leverage technology and data.

As we move forward, healthcare leaders need to embrace this change and invest in modern access control systems and integrations that can meet their specific needs. The time to act is now. Start by evaluating your current systems, identifying opportunities for improvement, and seeking out partnerships that can help you navigate this complex landscape.

If you are interested in topics such as this, consider joining the ever-growing community of the Access Control Executive Brief where members like HiveWatch, TDSi, and 4S Security engage, learn, network, and contribute to the next evolution and generation of the global access control industry.

LEE ODESS

Lee Odess is a globally recognized leader and influential voice in the access control industry. As a business analyst, community builder, consultant, and engaging speaker, Lee challenges conventional thinking, redefining the role of access technology in today's connected world. With a vision focused on holistic experiences, Lee advocates for the idea that security extends beyond the front door. He believes in empowering spaces to ensure safety, convenience, operational efficiency, revenue generation, and innovation. Throughout his distinguished career, Lee has guided owners and operators in harnessing the latest technologies to achieve secure access, exceptional user experiences, and future-proof infrastructures.

The Evolution of Advanced Security Technology for Healthcare Security

Healthcare security professionals must ensure that any strategic plan accounts for expansion and flexibility

Ben Scaglione

The past five years have seen a major evolution within the healthcare physical security space. Dramatically changing how healthcare security professionals conduct business today and in the future. The *first* evolution is the advances in security system technology. Security systems advanced technology can now truly integrate disparate systems making for easier use and greater data gathering and analysis. The *second* is the insertion of AI into physical security systems. AI is revolutionizing the physical security space by changing what we can see, how we see it and the prediction of adverse events. *Third*, is the revitalization in the use of physical security systems within the healthcare industry. Covid highlighted the importance of physical security systems within the healthcare setting and the continued examination of technology to help resolve current issues residing within the healthcare industry.

ADVANCEMENTS IN SECURITY TECHNOLOGY

Security technology systems have advanced, providing tools that help the healthcare security director better protect patients, visitors, and staff. Advanced technology systems can now detect and identify specific types of sounds. For example, raised voices. The escalation of an argument or fight. Alerting security of a potential event in the Emergency Department, the ICU waiting area or anywhere a video camera is present. Systems can determine gunshots. Specialized systems can detect the discharge of a gun and ever distinguish the types of guns being discharged.

Integrated technology can pinpoint locations and track people who have discharged a gun. Electronic security systems can now integrate with other

disparate systems. Combining access control, with video management, visitor management, infant protection, computer-aided dispatch systems (CAD), or incident management systems, to name a few. Better tracking inventory for keys, cards, security and hospital equipment, vehicles and cameras, card readers and all other physical security devices.

AI has become a major component of physical security technology and has transformed the healthcare security industry in several distinct ways. AI has expanded the ability of video surveillance through the improvement of object recognition. Systems now can detect specific objects like weapons and alert security of the event as well as track persons throughout the healthcare facility. Whether it's patient elopement or an infant abduction, AI has expanded the ability to track persons and things. Now detailed descriptions or photos can be loaded into the video management software and the software can search all cameras to find the person in question.

This can be done not only in recorded video but in real-time, live video. AI can find and track specific vehicles based on license plate number, make and model of the vehicle or vehicle color. Video systems can determine people who are loitering, like individuals who are hanging around building entry doors or the entrance to the Emergency Department or Maternity units. As stated earlier, distinguish sounds to determine raised voices, gunshots, screams for help and even keywords. Through data analysis, AI can assist in predicting outcomes and analyzing efficiencies, helping to reduce the potential for adverse events and improving productivity.

COVID-19 AND ITS EFFECTS ON SECURITY TECHNOLOGY

COVID-19 exposed the need for security advanced technology within the healthcare setting. Many hospitals and other healthcare institutions relied on security technology to help in the Covid-19 battle. Primarily, hospitals, clinics and other off-site facilities relied on temperature screening and tracking systems to help monitor staff and visitor compliance. Visitor management systems were implemented to better screen and track visitors during Covid. CCTV cameras were added along with other security devices to restrict access to facilities so that all persons could be funneled into key temperature screening locations. CCTV and other security devices were also used to monitor entrances and exits to augment workforce shortages.

This reliance on security technology sparked new interest in its ability to not only provide institutional security but to enhance healthcare operations, solving some of healthcare's biggest problems. Supplementing workforce,

simplifying operations, and providing real-time data for Covid compliance. Today, healthcare institutions are looking for advanced technology to assist in the reduction of violence, track persons and provide access control so that staff, patients, and visitors feel safer.

ADVANCED SECURITY TECHNOLOGY'S GREATEST GIFT

The greatest gift that advanced security technology has given healthcare security is data analytics. It is the collection and manipulation of data that is the most impactful to healthcare security professionals. Today's advanced security systems along with AI can gather data from disparate systems, combine databases and manipulate the data to provide, never seen before, information that can help healthcare security directors work more efficiently, respond to incidents faster and better predict risks and threats to the healthcare institution. Having the ability to collect and merge data on visitor management systems, metal detector alarms, false alarms within burglar and infant protection systems, security system outages, unauthorized use of access control devices and monitoring of security systems to determine patterns and trends within the data set.

Better defining the highs and lows in patterns and trends within data and determining the exceptions within a normal or average data set. Providing exception reporting by identifying spikes in incident, video, and access control data. For example, identifying people who repeatedly appear in incident reports, within the visitor management system, violate access control protocols or continually loiter within high-risk areas.

THE FUTURE OF ADVANCED SECURITY TECHNOLOGY

How do these advancements help solve some of the pressing challenges facing healthcare security today and in the future? Advanced security technology will improve security department efficiencies. Determining efficiencies in security services and incidents through defined analytics. AI will continue to evolve providing better predictive modeling to determine the most vulnerable places and staff within the healthcare institution. It will help in determining directed patrol and post assignments within identified high-risk locations. Advanced security technology will be able to analyze security department financial and workforce data to continually recognize operational efficiencies. New security technology will assist clinical, operational, and security staff in the prediction and warning of potentially aggressive behaviors. Identify, track, and alert security and hospital staff to high-risk people. Patients attempting to leave or who are kidnapped, and identifying unauthorized persons who

enter or loiter around hospital property. People who are barred from the healthcare institution due to employment termination, visitor restrictions, or previous violent acts.

"Security technology systems have advanced, providing tools that help the healthcare security director better protect patients, visitors and staff."

Advanced security technology is the path forward for healthcare security. The advantages it provides today and, in the future, dramatically increase the potential to reduce violence and increase operational efficiencies. However, the key to the effective use of advanced security technology is understanding how it works and what advantages it has for the healthcare organization.

THE HEALTHCARE SECURITY DIRECTOR'S ROLE IN ADVANCED SECURITY TECHNOLOGY

Advancements in technology have brought an onslaught of new technology and AI-branded products into the healthcare security marketplace. Each has its own unique features and pricing structures. There are now many product options for healthcare security professionals to choose from, making the security technology market a very confusing place. Ensuring that the right products are purchased and work effectively for the organization is key to the successful application of the newest technology.

The issue with using advanced technology is not so much that the product truly works but the security director's understanding of the product and how it will resolve security-related problems within the healthcare organization. Security technology is advancing rapidly. Products continue to get better; AI is becoming more predictive and technology manufacturers are focusing more on providing solutions to help the healthcare industry.

For the healthcare security professional, the future is very bright. With the continued advances in security technology healthcare security directors will have greater ability to provide effective security services.

HOW TO MAKE TECHNOLOGIES WORK FOR YOU

So how can today's healthcare security directors best utilize and plan for the newest advanced security systems? To successfully utilize advanced security technology, security directors need to educate themselves on how these technologies work and determine how technology best fits within the healthcare organization. How advanced technology can solve the specific security and organizational

problems present within the healthcare organization? As difficult and confusing as it can be, learning about the different available technologies, how they work, and where each company is going in the future is paramount to selecting and using advanced technology security systems.

Often, because of the lack of education, many healthcare security directors rely on integrators to choose the technology and products their institution uses for security systems. With the rapid advancements in technology and the constant growth and development of these products, many integrators may not understand a specific product or its full potential in resolving a healthcare institution's security problems. It is imperative that as professionals, healthcare security directors focus on educating themselves on the newest advanced technology products. Speaking directly with manufacturers or product representatives is one way to obtain information on a particular product or system.

"This reliance on security technology sparked new interest in its ability to not only provide institutional security but to enhance healthcare operations."

Working with an integrator who understands technology and can offer a variety of product solutions within their portfolio is another. Additionally, healthcare security directors need to work with leading publications and conference administrators to provide more technology education that is not based on profit, quota, or commission, but based on educating the end user.

Because of the complicated nature of advanced security technology and understanding what products work best for your institution, another option for the healthcare security professional is to hire a security technology consultant. An individual or group of people who understand multiple products and work closely with manufacturers to understand how they work and what the best application for their products might be. This is especially true when a healthcare institution is making a major change in its security systems. For example, changing out an old access control system throughout the entire organization, looking to integrate video management into an existing access control system, or when designing a security system for new construction or a major renovation.

In planning for this change, it is important to leave money in the budget to hire a qualified consultant. The consultant will work with the security director to determine what products work best for the healthcare institution and the security department. The consultant will be able to lay out a plan

of action for the installation of the systems along with budgetary requirements. This is especially important when a healthcare organization has limited financial resources.

For example, upgrading or purchasing a new access control system or video management system can cost up to a million dollars depending on the size and complexity of the installation. Laying out a plan that can install the new system over several years can help to manage costs, allowing the security department to obtain the new security technology they desire. However, this process must be accomplished correctly for the new or upgraded system to be installed and operate properly.

A consultant can also provide a master or strategic plan which can outline a physical security and financial plan over two to ten years. Many security technology consultants can also provide design services creating as-builts and architectural drawings. These attributes can help the healthcare security director obtain the systems they need to resolve some of the security problems existing within the healthcare organization.

CONCLUSION

The evolution of advanced security technology is on. Providing a bright future for the healthcare security director. The success in using the new technology resides in the healthcare security director's ability to understand the technology and how it best fits within the healthcare institution. Continually keeping abreast of the newest innovations and influencing publishers and conference administrators to provide education on advanced security technology is key to successfully implementing and utilizing the newest security technology. Picking the technology that best suits the healthcare institution and can help to resolve some of the pressing problems that are plaguing today's healthcare organizations. Ensuring that transformation to the newest technology is well thought out and planned from a financial and operational perspective.

Bernard Scaglione

Bernard J. (Ben) Scaglione is an experienced healthcare security professional with over 39 years of security experience, and 35 years within the healthcare environment. He has obtained his master's degree from Rutgers University School of Criminal Justice and is a certified security practitioner. He is a Certified Protection Professional, Certified Healthcare Safety Professional, and Certified Healthcare Protection Administrator. He is an accomplished Green Belt and Incident Command Exercise Designer. After a storied career as a security director with top healthcare organizations in the New York area, Ben now works designing security systems and conducting risk assessments in healthcare security for Ross & Baruzzini,

How Incident Management Software Can Enhance Healthcare Security

Healthcare organizations that don't have the right solutions in place will find it difficult to respond effectively in an emergency

Terry Swanson

For any healthcare organization, delivering excellent patient care is a top priority, but creating a secure facility is an often overlooked aspect of achieving that goal. Being able to plan for potential incidents, notify the right people, and actively manage events lets hospital staff know that their safety and their patients' safety are being prioritized so they can focus their efforts on delivering excellent care. However, if healthcare organizations do not have the right tools in place, it can be difficult to respond effectively when an emergency occurs. Incident management software can be a powerful solution when appropriately deployed as healthcare organizations look to combat multiple threats that may disrupt operations. Here are some ways healthcare organizations can achieve holistic security at their facilities with incident management software.

PLAN FOR POTENTIAL THREATS

To effectively leverage incident management tools, healthcare organizations need to understand the threats that can occur that would harm people or disrupt operations. Depending on the size of a facility, its location, and the services it provides, threats may vary, which is why it is important to bring together a group of representatives from different departments who can provide perspectives on various security and operational concerns. These issues can range from violent intruders to severe

weather that may impact staffing, but the more comprehensive a list that is created, the better prepared an organization will be. With the list in hand, organization leaders can then determine workflows for addressing threats and messaging to best communicate to staff, patients, and visitors what is happening and what steps they should take to stay out of harm's way.

Advanced planning can make an incident management tool more effective. It is less likely critical steps are missed in building out messages and procedures, and it helps reduce the workload when an incident occurs as every step has already been thought through.

DETECT POTENTIAL THREATS

Multiple tools are available that healthcare organizations can connect with their incident management software to help detect threats and initiate the management process. Panic buttons are a quick and effective way to signal that an issue is taking place and in healthcare environments, and multiple types of panic buttons may be needed to ensure easy access. Wearable devices can be given to each staff member, helping to reinforce that their safety is a priority. These devices can be engaged when dealing with difficult patients are when someone sees suspicious or violent activity ina facility. Physical panic buttons can be mounted in patient rooms, hallways, or other high-traffic areas. Keyboard shortcuts can also be configured at nurses' stations and mobile apps can be used by staff whether they are within a building or nearby and need assistance. This can be particularly helpful if staff are working odd hours and need to walk alone to their car in a space where help is otherwise not readily available. Panic button apps can share their location and give them direct access to security teams via a phone call until help arrives.

Panic buttons offer a powerful manual method for detecting threats, but automated methods can provide even more advance warning for a healthcare organization looking to minimize the impact of a threat. Incident management systems that monitor feeds from the National Weather Service can give healthcare organizations advanced notice about severe weather events that may impact operations or cause an influx of patients. Sensors can be connected to detect spills, hazardous materials, and air quality, and AI video surveillance can send alerts when a gun is drawn or other suspicious or dangerous activity occurs. This speeds up the alerting process so staff can intervene quickly before situations get out of hand.

"Once an alert has been initiated, the right people must receive it in the shortest amount of time."

DELIVER ACTIONABLE NOTIFICATIONS

Once an alert has been initiated, the right people must receive it in the shortest amount of time. In some cases that may mean sending an alert throughout an entire building, and in others, it may only require alerting specific teams, like security personnel and administrators. Incident management systems that offer the ability to designate groups and zones for targeted messaging can help ensure messages are delivered to the right people at the right time. It can also help restrict messages to relevant areas, avoiding sending sensitive messages to areas like visitor lobbies that may not need to be notified.

Those messages need to spur people to action so they stay out of harm's way. That can only be accomplished if messages reach them immediately. Robust incident management systems offer multi-channel alerting to reach people wherever they are with intrusive messaging that grabs their attention. With the ability to integrate with existing technology in a healthcare facility, including desk phones, desktop computers, digital signage, IP speakers, paging systems, and mobile devices, organizations can deliver text, audio, and visual messages that are impossible to ignore, getting information into the hands of the people who need it the moment they need it.

MANAGE EVENTS FROM START TO FINISH

Once an event has occurred and notifications have been sent out to alert others, healthcare organizations need to manage the event to bring about a successful resolution. This is where incident management software has an advantage over other alerting tools. While being able to share information is helpful, critical incidents are complex events and need sophisticated solutions to handle them. With incident management, healthcare organizations can plan for every step of a crisis and have those steps readily available to help minimize confusion and speed up the response process.

This can include prebuilding specific messages for different stages of an event, from an initial alert and follow-up details to the final "all clear" message. In addition, specific messages can be sent to key stakeholders asking them to join virtual incident response rooms so they

can assess the situation and determine the best course of action. Stakeholders can use resources they upload into their system, like floorplans, safety checklists, and links to camera feeds. They can also view real-time insights from their constituents by sending out notifications that ask for a response to determine who is safe and who needs assistance.

Each of these components can help healthcare organizations have a better understanding of the situation as it unfolds so they can better direct resources to help those in need and reduce the impact of daily operations.

RESUME NORMAL OPERATIONS

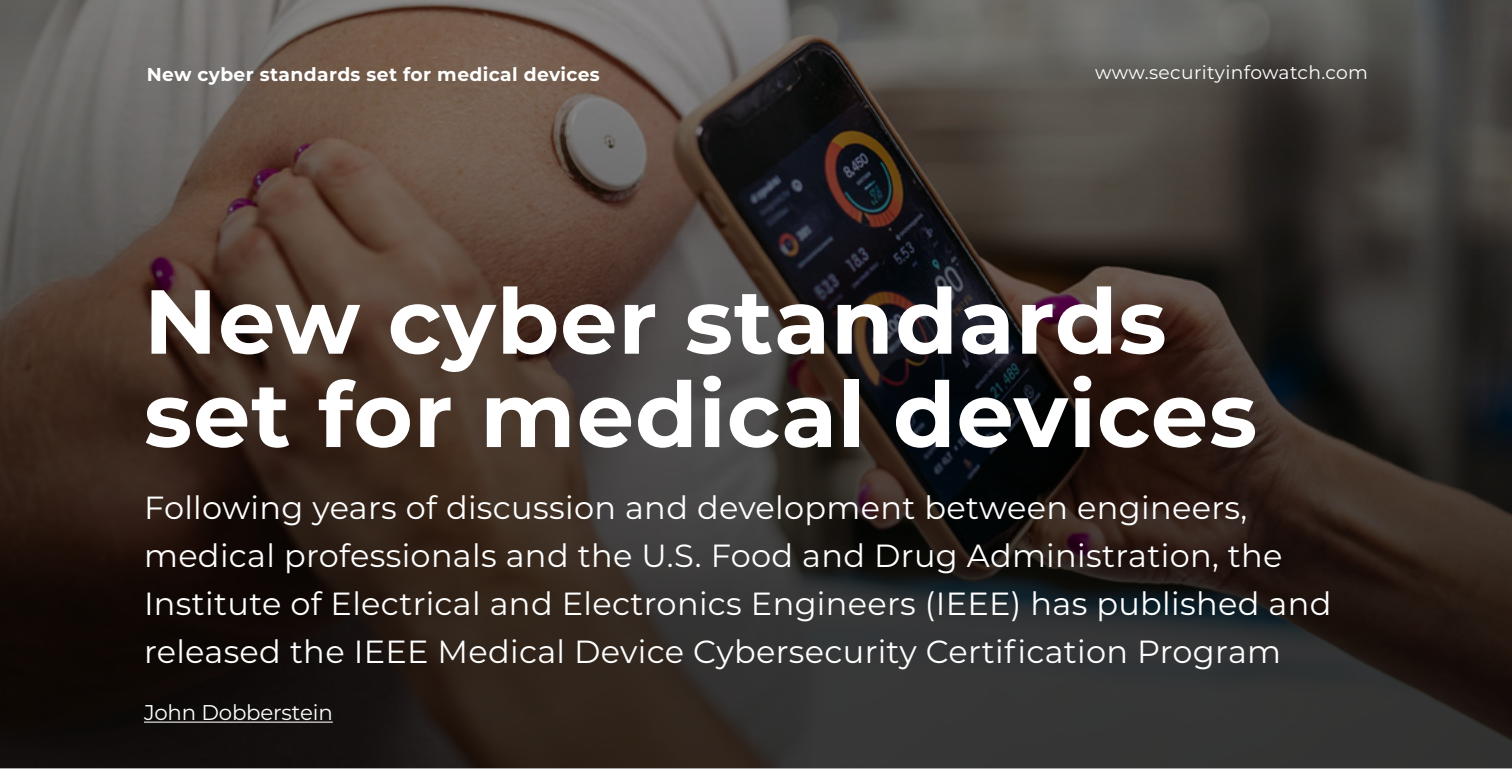
Part of being able to deliver excellent patient care is persevering in the face of a security threat. While certain activities may need to be paused to address an event as it happens, being able to get back up and running quickly enables a healthcare organization to continue to serve its patients with the best possible care.

Having pre-built messages and multichannel alerting means that organizations can let their people know that the danger has passed the moment it is deemed safe to resume normal operations. This can significantly reduce downtime by getting people back inside buildings and returning to work.

While it is impossible to anticipate every security issue that may arise within a healthcare organization, some steps can be taken and tools can be implemented that will simplify and speed up response times to help deal with a situation when it occurs. Incident management software can provide a rich, customizable toolset for healthcare organizations to plan for and actively manage incidents. With strong incident management strategies in place, organizations can create a secure environment focused on delivering exemplary patient care.

Terry Swanson

Terry Swanson is the president and CEO of Singlewire Software. Terry oversees the development of mass notification and visitor management software solutions. Before that, they were the President and CEO of OneNeck IT Solutions, focusing on optimizing the performance of custom IT solutions for customers. Terry also served as the Senior Vice President of Solutions Providers at OneNeck before becoming CEO. Terry has extensive experience in the IT industry, with a focus on solutions and sales leadership.



New cyber standards set for medical devices

Following years of discussion and development between engineers, medical professionals and the U.S. Food and Drug Administration, the Institute of Electrical and Electronics Engineers (IEEE) has published and released the IEEE Medical Device Cybersecurity Certification Program

John Dobberstein

Cyberattacks and data theft are a serious problem in many industries, but in healthcare the consequences could be physically dangerous or even deadly or enrich the pockets of bad actors on the dark web.

Following years of discussion and development between engineers, medical professionals and the U.S. Food and Drug Administration, the Institute of Electrical and Electronics Engineers (IEEE) has published and released the IEEE Medical Device Cybersecurity Certification Program.

The program provides a framework for medical companies to have devices tested to meet rigid cybersecurity standards and earn a certification label. The driving factor early on for the standards was the White House's cybersecurity directives issued in 2021, which among other things, pressured the FDA to increase protection of medical devices.

The first medical devices from companies, including Ascensia, have been certified under the new IEEE Medical Device Cybersecurity Certification Program. Test facilities from atsec in Sweden, Germany, and the U.S. have been officially recognized under the program.

DRIVING CONFORMITY

By submitting medical devices for IEEE certification, manufacturers can demonstrate conformity with an international standard. Having their devices evaluated against a rigorous test plan and checklists by IEEE authorized third-party test labs helps to ensure conformance with the IEEE 2621 standard. This may expedite the approval process by regulatory bodies.

IEEE and the IEEE Standards Association (IEEE SA) launched the program in 2023 as a result of the work done by the IEEE 2621 Conformity Assessment Committee (CAC), composed of stakeholders such as manufacturers, clinicians, the FDA, test laboratories, cybersecurity solutions providers and industry associations. It aims to help address cybersecurity risks in medical devices that capture and manage user bio data and impact quality of life.

Atsec labs in Danderyd, Sweden, Munich, Germany and Austin are the first to be officially authorized to test medical devices under the IEEE Medical Device Cybersecurity Certification Program.

"We enthusiastically embraced the opportunity to become a player in this domain when IEEE first contacted atsec in July 2022," said Sal La Pietra, President and co-founder of atsec information security. “We're particularly proud of this achievement because it follows the successful completion of two pilot projects that used the IEEE 2621 standard for medical device testing. These projects allowed us to refine our processes and demonstrate our expertise in applying this standard," added Rasma Mozuraite Araby, CEO of atsec AB in Stockholm, Sweden.

THE FIRST RECALL

One of the driving forces behind the new standard was Dr. David Klonoff, Medical Director for, Diabetes Research Institute at Mills-Peninsula Medical Center in San Mateo, Calif. A growing number of people with diabetes are turning to connected diabetes devices (CDDs) to monitor and manage their condition in an automated fashion, with wireless automatic transfer of data and treatment commands.

CDDs include blood glucose monitors, continuous glucose monitors, insulin pumps, smart insulin injection pens and automated insulin dosing systems.

For example, data generated by a continuous glucose monitor is wirelessly transmitted to an app on a smartphone, smartwatch or other devices, or to a cloud platform. Not only is this device used to issue alerts when glucose levels are out of range, but the continuing flow of data enables patients and healthcare professionals to see trends and patterns, which provide a more complete, nuanced picture of an individual’s status, Klonoff has noted.

For automated insulin dosing systems, the data is also used to direct a CDD worn by the patient to dispense insulin in controlled amounts at certain times.

In 2019, the FDA warned patients and healthcare providers that certain Medtronic MiniMed insulin pumps were being recalled because of potential cybersecurity

risks. It was the first time a connected diabetes device has been voluntarily recalled by a manufacturer because of cybersecurity vulnerabilities, Klonoff wrote in an article published in the Journal of Diabetes Science and Technology.

“The outcome could be life-and-death type situation. If a cyber attacker were to go in and try to adjust your insulin levels, you could have a very, very bad outcome as opposed to someone hacking your credit card account, which is equally bad, but no one's going to die from that,” says Ravi Subramaniam, Acting Senior Director for Global Business Strategy and Intelligence at the IEEE Standards Association.

EMBRACING THE STANDARD

“There have been number of cases when the medical devices were hacked, but nobody really wants to talk about it. This is really not good news for the industry, for the manufacturers or for the patients,” adds Ted Osinski, Program Manager for IEEE Certification Programs. “I think the medical device manufacturers, by and large, have taken notice of it. They've started to insert cybersecurity precautions in the products, starting from the design. Now they have consultants on staff. They know the future of the company depends on that. And so when they come to us, they usually, you would say they're prepared.”

IEEE does not guarantee a device manufacturer that collaborates with them will get FDA certification, Osinski notes, but the organization can help manufacturers prepare for the stringent FDA submission and certification process, which takes 2-3 months.

The test labs inform the device manufacturers what materials to submit, with the most important one being a document called the security target. From there the lab begins testing the product and working with the manufacturer to discuss the results and what additional safety steps may be needed.

There are three levels of testing based on the type of device and its criticality based on patience outcomes. IEEE evaluates the test reports and if they are satisfactory, IEEE issues a certification mark for the devices and places it on a registry.

Labs who want to be part of the program also go through an IEEE audit process, where the organization performs an onsite evaluation of facilities and lab capabilities and also evaluates personnel performing the testing.

The certification is good for three years, but if there are changes to a product it could require recertification or even a retest. The registry also includes the

software version tested, and any changes could trigger a recertification requirement.

The FDA can also refuse to accept a device that does not have cybersecurity features in it, which Osinski and Subramaniam say is a critical change because that wasn't done before.

The testing labs themselves must be re-audited on their certification with IEEEE every two years.

"The threat conditions continue to evolve day to day. Attackers are very, very sophisticated," Subramaniam says. "Our test plan and the standard helps the industry to even go beyond the daily change in the threat landscape. It really allows you to analyze the security target at what level of threat there is and perform the testing based on that."

Subramaniam believes the IEEE program will be embraced by the medical industry because it will be one international standard to follow, as opposed to trying to please regulators from every country they do business in.

"It also resolves a lot of headaches for the regulatory agencies that are struggling within their own region. Not to say that this program is going to address every single region's concerns, but at least it could be sort of general layer and then the regions may have more specific requirements themselves," Osinski says. "But it really helps to reduce the burden, the cost and time needed to get the product into the market."

Mercy Prescribes Security Screening to Address Clinical Staff Safety Concerns for Its Emergency Departments

The state of violence in the healthcare industry and within each hospital's community were considered when assessing their security policies

Delivering Healthcare Where It Is Needed

Founded in 1986 by Sisters of Mercy, Mercy has more than 42 healthcare facilities in Arkansas, Kansas, Missouri, and Oklahoma.

Over 40,000 doctors, nurses, caregivers and other staff provide care to millions of patients annually.

As a Catholic-based ministry, Mercy locates its healthcare facilities in areas where healthcare is needed. Adam Whitten, Mercy's Vice President of Operational Excellence, explains: "We bring healthcare to those who need it, when they need it, and where they need it. You won't find Mercy putting hospitals in areas where it is most lucrative. We put them where they are most needed."

A central mission of Mercy is to ensure that patients and visitors feel as safe and secure as possible when visiting one of Mercy's facilities. It is also critical that hospital staff, or coworkers as Mercy refers to them, can provide care to patients in a safe environment.

A central mission of Mercy is to ensure that patients and visitors feel as safe and secure as possible when visiting one of Mercy's

facilities. It is also critical that hospital staff, or coworkers as Mercy refers to them, can provide care to patients in a safe environment. "Our patients, family members, and staff need to feel secure because everyone who is entering has gone through the same processes to ensure that no one brings a weapon into one of our facilities that they could use to harm themselves, one of our coworkers, or another patient or family member of a patient," Whitten says.

FAILURES OF REACTIVE SECURITY SCREENING

The state of violence in the healthcare industry and within each hospital's community were considered when assessing their security policies.

"The unfortunate prevalence of gun violence, coupled with the fact that more people carry firearms, puts our public at an increased risk of violence," quoted Mercy's Executive Director of Public Safety Jon Belmar when stating why he looked at weapons screening systems for the hospital. "Healthcare settings are not immune to such threats, and after an incident where a weapon was brought into an Emergency Department, we decided we needed to do something."

Dr. Mark Griesemer, Mercy's Medical Director for the Emergency Department in Springfield, recalls the previous security process: "The lack of security created an environment subconsciously for patients and their families—whether it was in the exam room or waiting room upon their arrival."

Until recently, security screening was a reactive process at Mercy and something Mercy has been actively changing. "We look to our clinical providers, public safety officers, and technology partners to give us advancements—enabling us to be proactive versus reactive in every situation," comments Belmar. John Spier, an RN and Clinical Manager for the Emergency Department at Mercy's Hospital in Springfield, Missouri, agrees: "Individuals who enter our facility have a high priority, especially those in the Emergency Department. It is my responsibility to make sure safety questions are answered. We have individuals who can intervene appropriately and in situations where we need to de-escalate patients, family members, and coworkers to diffuse situations before they become a bigger threat."

PRESCRIBING PROACTIVE SECURITY SCREENING WITH EVOLV

Considering the above, Mercy searched earlier this year to identify a technology that would create a safer environment while not inhibiting patients from getting care.

As a result, Mercy Public Safety Leaders "...ruled out metal detectors - both walkthrough and hand-held wands - and x-ray machines from consideration right

out of the gate for several reasons. Aside from being highly inaccurate in discerning between nuisance and threat alarms, they require a high volume of staff to operate and cannot accommodate bariatric wheelchairs and gurneys."

"Standard walk-through metal detectors are not conducive to a care environment for multiple reasons. They hinder normal pedestrian traffic, allowing only one person to go through at a time. With the Express, we can have multiple people enter the system together and successfully screen all at once," says Whitten. "With Evolv, our patients and visitors do not need to empty their pockets or keys, phones or coins nor be subjected to follow-up searches that a metal detector would necessitate. Our officers can also man the Evolv system with one person versus the two to three necessary to efficiently utilize a standard metal detector."

Dr. Griesemer concurs with Mercy's new direction in security: "The Evolv Express is fantastic because it creates an additional safety net and raises the conversation around individual safety and others in the emergency department. It makes it easier for our public safety officers to do their jobs and identify those people who may have something on them."

Patients come to the Emergency Department with heightened anxiety and awareness. They often aren't certain what to expect. "The Express system assures them that we take their safety and security seriously," Belmar says. "And if they do have a weapon on their body or in their bags, we want the detection and screening to be as seamless and unintrusive as possible."

Until recently, security screening was a reactive process at Mercy and something Mercy has been actively changing.

EMERGENCY DEPARTMENTS TARGETED FOR INITIAL DEPLOYMENT

When determining where to deploy the Evolv Express systems, Mercy concluded that the entrances to the Emergency Department would be the best place to start.

Mercy looked at years' worth of hospital, community, and industry data to formulate his approach on where and how to deploy. "We went back through

our incident logs, not only to see how many events of workplace violence took place but where they occurred," Whitten says. "The vast majority occur in our Emergency Departmental and Behavioral Health areas. There is a precipitous fall off from there. We also know that after a certain time of night at most of our facilities, the Emergency Department becomes the only access point to the entire hospital. All other doors are locked and guarded so no one else can come in."

With these two factors in mind, Mercy decided to begin the rollout of the Evolv Express systems at Mercy's Emergency Departments—and they began with the Springfield location. An Evolv Solutions Engineer worked alongside Mercy's security team and safety officers at the Springfield hospital to set up an Express single-lane system at the entrance to the Emergency Department. This included integrating Express operating procedures into the Public Safety team's ConOps documentation.

The Evolv Solutions Engineer also trained the team on using the system, particularly how to differentiate between alerts on wheelchairs and gurneys versus potential weapons. "The Express is very easy to learn and use," Belmar says. "The Evolv team did a great job of training our security guards at each of our hospitals where we rolled them out. We are up to eight locations now, and we plan to continue adding them to locations where it makes sense."

The Express system is also designed to comply with the American Disability Act. Each lane is 39.8 inches wide; wheelchairs and gurneys easily fit through the Express Lane.

When it came to the first day of deployment at the Springfield location, Mercy admits they were a bit apprehensive. "With any new technology, you're always looking for the red herring," Belmar says. "Our officers test the system for proper function daily. It is easily, quickly tested, and calibrated to ensure it functions as designed."

USING EVOLV INSIGHTS ANALYTICS AND CORTEX AI FOR GREATER EFFICACY AND EFFICIENCY

Advanced capabilities in the Express system are something Mercy is especially excited about.

"We use Evolv Insights to look into details around how many people come into each of our Emergency Departments and at what time of the day or night," Belmar said. "We look at how many weapons we find per location and how many alarms we get. We report these to the leadership team to demonstrate how we keep our facilities safe and the value we get from our Evolv investments."

Artificial intelligence and machine learning are additional factors that Mercy finds particularly useful. "Evolv Cortex AI allows us to work with the Evolv team to constantly help the Express systems to learn and become more and more accurate in screening patients, visitors, and staff," Belmar says. "With enough data, the Express system may eventually learn to distinguish between gurneys and wheelchairs, tumblers, and canes versus weapons."

Mercy looked at years' worth of hospital, community, and industry data to formulate his approach on where and how to deploy.

RESPONSE TO THE EVOLV EXPRESS SYSTEM

The response from everyone involved in Mercy's Emergency Departments where the Express systems have been rolled out has been very positive.

The Clinical staff in each Emergency Department have been just as excited about adding the Express. "We were hearing a lot of concern from our Emergency Departments post-DePaul, post-Tulsa about our safety," Dr. Griesemer recalls. "We were asking them 'What are you doing to make us safe? How can I feel safe treating patients?' These concerns went away at every location where we have rolled out an Express system." Dr. Griesemer adds, "Safety for me, as both a physician and medical director, means a lot of different things. We can focus on caring for patients rather than worrying about them carrying and using it on the staff. At the same time, the Express gives our patients and families a feeling of safety and security—which is important for anyone experiencing a health event or a loved one experiencing one."

Patient and visitor reaction to the Express systems has been positive as well. "I was worried about secondary screening checks with patients and family members," Whitten recalls. "My concerns were unwarranted. The Express system pinpoints the area of a potential weapon with a red box. It allows our safety officers to avoid extensive checks of a patient's or family member's bag or person. People who carry a firearm are conscientious about doing the right thing. In most instances, they forgot they were carrying and are apologetic and quick to fix the issue."

For patients or family members with mental health disorders, Whitten explains that the

Evolv system enables the Public Safety team to focus on a particular area of the person's body or bag rather than performing a full screening—something that could exacerbate certain situations. "Evolv is not a metal detector; it is a weapons detection system," Whitten adds. "It helps reduce the risk and presence of weapons on our campus and helps us enforce our weapons-free policy."

SECURITY STAFFING SAVINGS WITH EVOLV OVER TRADITIONAL METAL DETECTORS

The differences between the staffing resources required to manage an Express system and those needed for a traditional metal detector are dramatic.

"We would need 12 full-time security guards to manage a walkthrough metal detector versus 4.2 full-time security guards for Evolv," Mercy's security team notes. "When you look at the Evolv system, you're really talking about something less expensive, less intrusive, and more efficient to operate."

While this is a substantial operational gain for just one Emergency Department, the full-time staff savings multiply quickly for Mercy as Express systems are rolled out to more Emergency Departments. Had Mercy used walkthrough metal detectors or x-ray machines rather than Express systems, it would have needed to hire an additional 62 full-time safety officers.

EVOLV EMPOWERS CLINICAL STAFF TO FEEL SAFE WHILE MINISTERING TO PATIENTS IN NEED

The Express deployments have delivered great results for Mercy.

At some of the Emergency Departments, such as the one in St. Louis, Missouri, Mercy screens up to 1,000 people daily. "Our officers have found multiple concealed firearms and knives that otherwise could have entered our facility," Belmar says. "We have even encountered one patient with four firearms and multiple knives in a backpack."

Spier summarizes what Evolv means to him and the Springfield Clinical team: "Evolv is a safety net for all of us. It lifts the burden off the shoulders of coworkers, empowering them to treat patients while continuing to feel safe, knowing the Evolv reduces the potential for harm to both coworkers and patients served."

"Nobody can control human nature," adds Whitten. "But if we can control certain areas of our campuses to ensure that we're providing the best and most secure environments possible, then we are doing what we need to do—and the Evolv system is an important linchpin in making this possible."

Contact us to learn more about helping to create safer zones where you live, learn, work or play.

info@evolvtechnology.com

+1 781.374.8100