Identity and Access Management for Healthcare

What Health IT Security Leaders Should Expect

PROVIDED BY

healthcare innovation
PEOPLE. PROCESS. TECHNOLOGY TRANSFORMATION.

IN COLLABORATION WITH

imprivata®

A seamless IAM solution for healthcare organizations offers potential for productivity, security gains.

Ten years ago, most health system information technology leaders did not have Identity and Access Management (IAM) at the top of their priority lists. Provisioning and de-provisioning new clinicians so they could begin seeing patients was primarily a manual operation, done by IT staff. But today most Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) recognize they need a detailed and sophisticated IAM strategy. So, what changed?

First of all, the federal HITECH Act of 2009 provided subsidies for more providers to implement electronic health records (EHRs), so the number of hospitals and physician offices with EHRs skyrocketed. Clinicians began using many other digital systems connected to the EHR. These investments in health IT meant clinicians were faced with multiple log-ins, which, over time, can contribute to physician burnout. Easing that process with single-sign-on capabilities helped spur the growth of IAM solutions. In addition, the Meaningful Use reporting requirements tied to those EHR subsidies, as well as HIPAA security requirements, meant that IT teams had to start thinking about their ability to verify and track who had access to which applications and data, which led them to consider multi-factor authentication.

CIOs and CISOs realized they had to be prepared for audits to ascertain that employees who had access to protected health information (PHI) had the proper permissions. But did they even know who had access to PHI or a way to determine if they should have access?

Many health systems had avoided doing the necessary identity governance work because it can be difficult and time-consuming. It requires IT to build a relationship with colleagues in human resources to determine employee roles from job descriptions and assign software application access permissions to those roles. Unfortunately, a health system could have twelve thousand positions and five thousand job descriptions. Narrowing those down and defining roles requires observation and analysis. For instance, it might require studying the applications that a few pediatric nurses have access to, creating a definition of the software required for that role and allowing all other pediatric nurses to have access to those applications.

Cybersecurity threats on the rise

In addition to ever-changing federal regulatory requirements about auditing access to sensitive health information, the rise of cybersecurity concerns, including ransomware,

insider threats and vulnerabilities related to connected medical devices, has put pressure on IT and security executives to up their game.

In 2017 the U.S. Department of Health & Human Services convened a healthcare industry cybersecurity task force, which issued a report making several recommendations, including requiring "strong authentication to improve identity and access management for healthcare workers, patients and medical devices/EHRs."

Stating that the delivery of healthcare is founded on the establishment of a trust relationship between and among providers and patients, the task force noted that the foundation of this trust is the belief and confidence in the identities of the individuals involved (providers and patients). "Through strong identity and access management practices, this trust relationship should be extended to the medical devices that are used to provide patient care," their report said.

The HHS task force described how clinicians in a hospital setting are required to access multiple computers throughout the facility repeatedly (up to 70 times per shift) as they deliver care to patients. "In order to authenticate their identity so that they can perform common tasks (e.g., access a patient's medical record, order diagnostic tests, prescribe medication, etc.), a clinician typically enters his or her user name and a unique password. This widely used, single-factor approach to accessing information is particularly prone to cyber-attack as such passwords can be weak, stolen, and vulnerable to external phishing attacks, malware, and social engineering threats."

Addressing 'Shadow IT'

One nagging problem that faces security officials who need to know the identities and roles of all the people connected the health system network has been labeled "shadow IT." This is when departments or individuals set up their own servers or deploy applications or cloud services without the direct oversight of the central IT organization.

For instance, a cardiovascular institute or radiology group could have its own servers and applications that are not tied into a hospital's Active Directory system. When someone who works in that group leaves the organization, central IT might have a good process for de-provisioning them out of Active Directory. But the "shadow IT" server in radiology may not "know" that a person has left the institution. Although the person no longer has Active Directory credentials, they might have credentials on a PACS (picture archiving and communications system). If they can still get access to the PACS system, they could use that to gain access to other parts of the system. Central IT might not have assurance that people who were provisioned have been properly de-provisioned from all the applications to which they had access. The perimeter back door is open for cyber-intruders.

In March 2019 networking vendor Cisco published the results of its CISO Benchmark Study of more than 3,200 IT security leaders from 18 countries. The report noted that health systems must look at what's happening inside as much as outside their organization, and be aware that some criminals can log in rather than break in. "This drives the need for better multi-factor authentication," the study noted. "Nowhere is the need more apparent for balancing the need for security (letting the right people in) with supporting seamless business (not hindering the people you do let in with a clunky user authentication experience)."

In Cisco's survey, only 54 percent of respondents said that, in their organization, "access rights to networks, systems, applications, functions and data are appropriately controlled." And only 53 percent said, "We do an excellent job of managing human resources security through employee onboarding, and good processes for handling employee transfers and departures."

Traditionally, most hospitals and integrated delivery networks have underinvested in IT security, so there is still a lot of room for improvement. A 2017 KLAS/CHIME benchmarking report surveyed close to 200 healthcare IT security leaders. Only 16 percent reported feeling that they have a fully functional security program. More than half of the organizations that are still developing their security program are spending less than 3 percent of their total IT budget on security. Also, 32 percent of respondents said that they have not implemented an IAM solution yet or are using a homegrown solution.

The KLAS/CHIME report also noted an evolution in titles and responsibilities for cybersecurity. Forty percent of organizations have a vice president or C-level in charge of their program. About half of these are CISOs; the other half are CIOs/CTOs. Their executive brief notes that "compared to those in an IT role, respondents with a security background more often report having a vice president or director (often a CISO or security director) in charge of their security program. They are also significantly more likely to have a cybersecurity framework in place and a deeper breach-readiness level."

The importance of a seamless solution

As these IAM teams move along their digital maturity journeys, they are starting to see the importance of seamless systems for identity governance, authorization and access control and focusing more holistically on the identity lifecycle. A 2017 Forrester Consulting research study surveyed 203 IT security decision-makers in North America. It found a correlation between implementing more IAM capabilities and a reduction in security incidents. The study also found that those with the most mature identity and access management stances "gravitate toward integrated platforms, which are solutions that allow them to consolidate multiple IAM technologies." The Forrester researchers

also found that higher maturity IAM companies are likely to see other benefits, such as increased employee efficiency and improved compliance with audits.

The 2019 Cisco survey results back up the idea that integrated solutions are becoming more important. In 2018, 21 percent of respondents had more than 20 vendors and 5 percent had more than 50. In 2019 that has fallen to 14 percent and 3 percent respectively. "We're finding the trend for number of vendors and solutions going down," the authors note, "but as multiple vendor solutions aren't integrated, and therefore don't share alert triage and prioritization on limited dashboards, our survey found that even those CISOs with fewer point solutions could better manage their alerts through an enterprise architecture. To better manage alerts, one best security practice is to reduce the number of vendors and point solutions."

This is where companies with a clear focus on healthcare are aligning with the needs of CIOs and CISOs for a true IAM platform rather than individual point solutions. "Whenever you have piecemeal solutions, you are going to have security gaps for the IT department to stitch together," says Barbara Dumery, Senior Vice President for Product Management at Imprivata, a leading IAM vendor in the healthcare space. There may be gaps from the clinician experience perspective, too — such as different authentication processes from each vendor. "Other IAM companies are not focused solely on healthcare. They work in a lot of markets, so they may not have the depth of knowledge of what is needed in this shared endpoint environment," she adds. "We like to think about that last mile of connectivity for the clinicians and healthcare workforce. When a clinician needs to be provisioned within or de-provisioned from the EHR, we are able to do that with our identity governance solution."

Health system executives want to make sure that IAM capabilities can work across all application types, including cloud business applications, and across an array of devices. "In addition to virtual desktops, they have to think about mobile phones and medical devices," Dumery explains. "The way we see digital identity in healthcare, it starts with identity governance. You have to have a way to provision and de-provision identities. Then you want to be sure that the right person is accessing data, so we have an identity-proofing solution. Because you want to be able to easily assure their identity, you need multifactor authentication comes in for access management. To make it all completely seamless for the healthcare workforce, we offer single sign-on so they can have easy access to all their applications." The last piece is that you want to have a self-service capability to manage passwords. "This is all part of an integrated IAM framework to ensure the IT department can have a single solution for all their users and all their needs."

Wes Wright, Imprivata's Chief Technology Officer, can draw on his experience as a health system executive to confirm the value of a seamless IAM solution. Before joining Imprivata, he was the CTO at Sutter Health, where he was responsible for technical services strategies and operational activities for the 26-hospital system. Wright, who also has served as CIO at Seattle Children's Hospital, recognizes the trend toward integrated

platforms and services. "We now have what I call a cradle-to-grave identity management and access system that we make sure is seamless," he says. "We have several reporting modules that can alert you if a person wasn't de-provisioned properly, or they were de-provisioned but their badge is still trying to access something. I think having a single integrated suite for IAM is a necessity, and my vision is that, three to four years from now, our customers will not be buying an Identity Governance product, a OneSign single sign-on product and a Confirm ID authentication product from us; instead, they will be buying a complete IAM service from Imprivata." The tight integration of those three solutions, he adds, gives users a more holistic view of their risk vulnerabilities.

Wright calls the fact that Imprivata focuses solely on healthcare the company's "secret sauce." Others may have a few people working in healthcare, but they don't have the depth and breadth of knowledge and focus, he says. "Our whole existence is healthcare. Not only do we have that integrated software suite and workflow insights, but we know which reports you have to have in place to meet regulatory requirements."

Jeffery Cooper, Director of Technology Services for Augusta Health, a community health system headquartered in Fishersville, Va., has dealt with several of the issues Wright describes. Augusta has had different groups assigning permissions to the inpatient and ambulatory EHRs, and another assigning permission to Active Directory and Exchange. It also has department ancillary consultants in cardiology and radiology that have dotted line reporting into IT, but provisioning was delegated to the individuals in those departments. "Part of what we are doing with Imprivata is creating a group called Access Management to pull those functions back into IT," Cooper says.

Cooper's team is working to have everything about provisioning and de-provisioning run through the human resources information system (HRIS). For example, for all nursing staff, they will get a daily report from the HRIS system fed into Imprivata Identity Governance. "Our intent is to map all these systems using Imprivata's bridge technology, mapping roles and responsibilities in the various systems we have, so that it automates provisioning the accounts," he explains. Cooper's goal is to have Active Directory, Exchange and the two primary EHRs automated within the next year.

For Cooper, it also is important that he reduce the number of vendors he works with in this space. "My overall goal is to have a single vendor and a single identity access solution," he says.

Electronic prescribing of controlled substances

Dumery offered the example of electronic prescribing of controlled substances (EPCS) as a use case in which Imprivata built an integrated solution addressing clinicians' efficiency needs and IT's compliance needs. In 2010 the U.S. Drug Enforcement Administration (DEA)

issued regulations for electronically sending prescriptions from prescriber to pharmacy. "We saw an opportunity to embed the authentication requirements within the EHR work flow," she explains. "We understood the benefit of providing end-to-end solutions that addressed all the regulatory compliance concerns, had the identity proofing tied to the authentication and tied into the workflow of the EHR. We saw how critical that would be."

Four-hospital NorthShore University Health System in Evanston, Ill., was one of the first health systems to tackle EPCS when it deployed Imprivata's Confirm ID in pilots using a fingerprint reader integrated with the EHR.

In a further step, Imprivata added hands-free authentication capability to EPCS. The first factor might be a password or fingerprint, and the second might be a push token on a mobile phone. "We are able to automatically retrieve that secure token from the phone via Bluetooth," Dumery explains. "It is still two factors of authentication and still meets DEA regulations, but is completely transparent to the end-user. That combination of an end-to-end EPCS solution for the end-user and hands-free authentication is really remarkable."

Continuing to work on productivity

When CIOs and CISOs make the case for investing in IAM, they stress both better security and improved productivity. Dumery notes that many health systems have not yet realized the productivity gains initially promised by EHR adoption. Yet they have to continue to combat increasing cybersecurity threats like ransomware, while constantly thinking about how to make their work force compliant in a way that is not burdensome to them. Connecting an IAM lifecycle solution with clinical solutions provides a solid foundation. "It gets back to focusing on the clinician experience," she says. "We are in a space to help organizations do this." Employees may not even realize they are being more secure; they just realize they are more productive, she adds.

> "IT departments tell us they have heard from clinicians that this is the first time the IT department did something for them as opposed to doing something to them. That is really powerful."

About Imprivata
Imprivata®, the healthcare IT security company, provides healthcare organizations globally with a security and identity platform that delivers ubiquitous access, positive identity management, and multifactor authentication. Imprivata enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience. Designed and purpose-built for healthcare, our Imprivata Identity Governance solution is an end-to-end solution with precise role-based access controls, automated provisioning and de-provisioning, streamlined auditing processes, and analytics that enable faster threat evaluation and remediation. For more information, please visit www.imprivata.com.