TWO FACTOR AUTHENTICATION AND DIGITAL IDENTITY MANAGEMENT
CONTRIBUTING EXECUTIVES

John Santangelo
Senior Director - Information Technology
Cleveland Clinic Florida

John Santangelo is a caregiver and proven executive leader in Healthcare Information Technology with a primary focus on building teams centered on developing and implementing technology to improve patient care. In John’s role as Senior Director, Information Technology, he oversees all aspects of information technology at Cleveland Clinic Florida including network services, clinical informatics, IT business systems, and telecommunications and telemedicine services. With over 16 years at Cleveland Clinic, he has led many large implementations and coordinated large system integration projects in conjunction with Cleveland Clinic Ohio.

John Christly
Chief Information Security Officer, NSU HIPAA Security Officer
Nova Southeastern University

John Christly is a seasoned Technology Executive and Cybersecurity expert with experience both domestically and internationally. He is an MSI Senior Fellow™ and has many years of experience in technical and cybersecurity related operational, project, and program management. His experience includes several industry regulations including HIPAA, HITECH, GLBA, FERPA, FCPA, FIPA, and PCI. As a highly accomplished author, Mr. Christly’s articles have appeared in publications such as Security Magazine, Executive Insight Magazine, 24/7 Magazine, and the ISSA Journal.

Sumit Sehgal
CISO
Boston Medical Center

Sumit Seghal is The Chief Information Security Officer for Boston Medical Center (BMC), and focuses on increasing strategic integration of existing information security programs with efforts relating to improvements in the area of business continuity and emergency management, as well as advanced threat detection and response. In this role, Seghal has Implemented BMC’s Identity and Access Management program, Lead the alignment of governance areas of business continuity and information security, Improved BMC’s information security threat response posture, and guided enterprise-level security strategies and initiatives across the organization.

Chandra Venkat
Sr. Manager
Cerner Corporation

Chandra Venkat is the practice manager with Cerner, and is responsible for oversight of strategic installations of the Cerner electronic health record platform. Venkat has extensive experience in the installation, strategic optimization, and data integration efforts behind Cerner’s enterprise EHR platform. Venkat has a Masters of Business Administration from the University of Kansas.

Benjamin Wyrick
Vice President of Sales - North America
Vasco Data Security

Benjamin Wyrick joined VASCO Data Security in 2005, and oversees successful managed strong authentication and digital identity management projects across North America. Wyrick is a sought after presenter at national security conferences, and focuses on the topics of preventing cyber fraud, account fraud, and transaction security for online and mobile applications.
TABLE OF CONTENTS

4 Executive Summary
5 Foreward
6 Strong Authentication
6 Multiple Systems
7 Single Sign-On
8 Authentication Tools
9 Awareness Grows
10 Digital Identity Management
11 Current Experiments
12 Patient Authentication
13 Clinician Authentication
14 EPCS Paves the Way
15 Health Information Exchange
15 Upgrading Older Systems
16 Ready for Change
17 Conclusion
18 Recommendations
19 References
FOREWORD

In the process of the digital evolution in health care, security of electronic protected health information (ePHI) has been frequently overlooked amid the complexity of hospital IT systems. So it comes as no surprise that in 2015, almost half of all serious data breaches were in healthcare, and the FBI has warned of more troubling times ahead.

As the Chair of the HIMSS Identity Management Task Force, I witnessed this evolution firsthand. I recall advocating for multi-factor authentication and identity management in healthcare from 2005 to 2008, only to receive blank stares in return.

HIPAA, HITECH, the Office of Civil Rights’ (OCR) “Wall of Shame”, ransomware, along with other industry policies and breaches have converted blank stares into a laser-focused attention on security, and identity proofing. By 2020, ONC expects that at least 50% of health care organizations will have implemented identity proofing and authentication best practices.

VASCO Data Security is proud to have partnered with Healthcare Informatics to produce this timely research report on authentication and digital identity management. We’ll hear from experts in the field regarding top strategies and the current state of security and identity proofing in healthcare.

We are all patients—and this report provides hope, perspective, and approaches to protect ourselves from our health records falling into the wrong hands.

Sincerely,

Michael Magrath
Chair of the HIMSS Identity Management Task Force
Director of Business Development, Healthcare
VASCO Data Security
EXECUTIVE SUMMARY

MIT gave birth to the computer password over 50 years ago, yet most healthcare organizations still depend on passwords for user authentication. But, with major security breaches increasing and cyber thieves focusing intensively on healthcare, this isn’t good enough. Even if an organization uses strong passwords or requires them to be changed frequently, they’re a very thin line of defense. According to one recent study, three-quarters of security breaches involve lost or stolen passwords, and it’s not uncommon for healthcare employees to share passwords with others.¹

John Christly, executive director and chief information security officer at Nova Southeastern University in Davie, Fla., says that password protection is outdated and poses unacceptable security risks. “It’s an archaic technology that should be extinct and shouldn’t be relied upon,” he says.

John Santangelo, senior director of information technology at Cleveland Clinic’s Florida branch, agrees. “Within a short period of time, passwords will get more antiquated as we move toward more e-services in healthcare,” he points out. “So it’s time to look for a new method based on an interoperability requirement and the mandates of healthcare reform.”

The obvious alternative to relying on passwords is two-factor authentication, which is widely used in banking but not in healthcare. Two-factor authentication employs methods such as smart cards, one-time password tokens and biometric devices, to ensure that users are who they say they are. Two-factor authentication using mobile devices is also becoming more widespread.

Many healthcare organizations seem to be reluctant to adopt this “strong” authentication because of its perceived cost and complexity, Christly notes. Moreover, it’s hard enough for clinicians to remember multiple logins and passwords—multiple two-factor authentication (devices) might be intolerably burdensome if they’re not done right.

Strong authentication, however, need not add more difficulties if it is combined with a new approach called “digital identity management.” In this model, which some healthcare organizations are already piloting, an individual is thoroughly vetted before receiving a digital identity. This digital identity includes a credential that is specific to that individual. Any organization that creates an “identity ecosystem” that includes the patient or clinician, can enable use of a digital credential and a second factor to authenticate him or her. So people do not have to remember multiple passwords to log into different systems as they move across the identity ecosystem.

This paper explains how strong authentication and digital identity management can increase health data security while making it easier for providers to do their work. We also explore how patients can use this method to view and download health records from multiple portals while increasing privacy protection.
STRONG AUTHENTICATION

Two-factor authentication adds an extra layer of security that healthcare organizations badly need, notes Santangelo. However, healthcare providers can be deterred by the complexity of some two-factor authentication tools. The Cleveland Clinic, for instance, initially had hardware issues with biometric devices, although the organization later overcame those challenges, he says.

Christly agrees that two-factor implementation can be challenging. He also doesn’t deny that it can be costly, depending on which methods are used. For example, smart cards require card readers that can cost $50 each, he says. “If you multiply that times thousands of workstations and remote users, it can be high cost. But there are ways to back into this.”

Some hospitals, he notes, already have card readers built into their computers. Also, two-factor authentication can be rolled out across an enterprise gradually over time. So these technologies doesn’t necessarily entail a big upfront investment, he says.

Benjamin Wyrick, vice president of sales and operations for VASCO, a vendor of data security systems, notes that costs vary significantly among different types of factors. For example, he says, “Fingerprint readers are costly solutions. But if you talk about face or voice biometrics, those are technologies that will see a higher rate of adoption, because they’re more cost effective for hospitals.”

MULTIPLE SYSTEMS

Another barrier to strong authentication, Santangelo says, is the decentralization of information systems in many healthcare organizations. That is not a problem at Cleveland Clinic, where most data either originates in the health system’s EHR or has been integrated with the EHR if it comes from outside systems. But many providers’ healthcare information systems are not that well integrated, he says.

“In some cases, providers need to authenticate to multiple systems, and the majority of organizations out there are struggling with that. They’re dealing with the integration of many systems and getting data from multiple sources, and each of those sources has its own authentication platform,” he points out. “That’s where it starts getting very complex, and where you get the obvious breaches where people are writing passwords on sticky notes or sharing their access with support staff to make their lives easier and to delegate certain restricted activities.”
It is possible to sidestep this challenge, Christly says, by making effective use of the “active directory” function included in the Microsoft Windows-based operating system on servers that are set up as “domain controller” servers. (Active directory, often used in conjunction with single sign on applications, includes the Lightweight Directory Access Protocol [LDAP], another authentication protocol called Kerberos, and the Domain Naming System [DNS].) When all the systems in a healthcare organization are tied to the active directory, and the organization uses two-factor authentication, it can help to protect the whole enterprise, he says.

According to Christly, EHRs are usually standalone systems that are not typically tied into a network’s central directory service. But in many cases, they could be connected, because “most EHRs support LDAP and active directory authentication,” he says. “So the hospital systems that plan for this as part of the initial implementation tie it into active directory when they implement the EHR. But I’ve seen way too many that leave them separated.”

Many legacy applications, however, do not support LDAP or active directory, notes Sumit Sehgal, chief information security officer of Boston Medical Center. “The integration of our systems with LDAP wasn’t matured until about three or four years ago, and our systems go back 15 years,” he says.

**SINGLE SIGN-ON**

Physicians and nurses like single sign on (SSO) systems that allow them to log in to all of the applications they need at the same time. Not only does this allow them to use only one login and password, but it also reduces the amount of time they must spend logging in. While some reports indicate that the majority of healthcare organizations use SSO, Santangelo doubts that many providers have fully deployed the technology. What deters them, he says, are security issues related to providing centralized access to multiple applications.

On the other hand, he adds, there are also security problems in requiring clinicians to remember multiple passwords for multiple systems. “The potential to compromise security at that level is greater than if you have it centrally managed and secured through one kind of portal. So there’s a lot of validity to SSO, but it’s difficult to implement it in a universal manner in a very complex environment where you have clinical and financial systems running.”

One of the vulnerabilities of SSO is the use of passwords. Consequently, Christly suggests combining SSO with two-factor authentication. Not only does that provide secure credentialing, but “it makes it very easy to use for the end users, who just want to get in and get out and not have to deal with complex logins and different passwords for different apps,” he says.

“Most EHRs support LDAP and active directory authentication. So the hospital systems that plan for this as part of the initial implementation tie it into active directory when they implement the EHR. **But I’ve seen way too many that leave them separated.**”

—John Christly
Boston Medical Center (BMC) has piloted SSO programs, notes Sehgal. Clinicians working in the hospital could use SSO during these pilots. So could staff physicians in their offices. But they couldn’t utilize SSO from home or any other remote location. In those locations, they had to use a portal and two-factor authentication to access the system, he says.

Sehgal believes that SSO increases productivity. “If clinicians spend five minutes signing on and they do it 20 times, that’s 100 minutes out of their day,” he points out. “SSO also works better for security because it allows you to change passwords on the back end if need be. It also allows you to control and change PINs, and it integrates fine with two-factor authentication.”

Without strong authentication, however, SSO leaves a large loophole for cyber thieves to drive through. Also, SSO is only applicable within a single enterprise. So its usefulness is limited for providers who move between care settings and those who need to access data from multiple hospital systems.

**AUTHENTICATION TOOLS**

More than 60 different types of factors are available for two-factor authentication. These can be categorized as something you have or something you are and always need to be combined with something you know in order to offer secure “two”-factor authentication. In the first class, for example, are hard and soft tokens and smart cards; in the second are thumbprint, palm, voice and facial recognition.

There are pros and cons to all of these approaches in the healthcare environment. Wyrick says hospitals are likely to use a variety of tools, depending on their needs. “Some segments of the market are going to use mobile—maybe an SMS one-time password or [mobile] push notification. Other segments are going to use hardware, because they don’t have these other technology tools.”

The healthcare executives interviewed for this report are divided on the best approach to two-factor authentication. Despite Cleveland Clinic’s technical problems with biometric authentication, for instance, Santangelo believes that biometrics are, “probably the most secure and functional way to do it. These tools provide a truly individual authentication method that doesn’t require you to remember something or carry something with you. You can use your thumbprint or other methods. That’s the future.”

In addition to thumbprint or facial recognition scanners in healthcare facilities, he notes, smartphones with thumbprint readers and cameras can be used for biometric authentication. “It needs to be refined a little bit, but the technology that’s out there is sufficient. Everybody is walking around with a device that could facilitate that kind of process.”

“If clinicians spend five minutes signing on and they do it 20 times, that’s 100 minutes out of their day.”
—Sumit Sehgal
Christly, in contrast, sees more negatives than positives in biometrics. “I’m not in favor of things like fingerprints or even retina [identification]. Depending on the area they’re being used in, those technologies can be very non-user-friendly and obtrusive. For example, if you’re in a sterile environment and you’re wearing gloves, a fingerprint reader is not necessarily the right solution.”

While biometrics could work in other healthcare environments, he says, a single strong authentication approach is superior to using different solutions in different areas of the organization, which he says is hard to support technically.

Some organizations have had good success in using hard tokens. “They seem to be universally acceptable,” Christly says. “Nobody likes carrying around a keychain token, but it works. And it’s something they have in their possession that typically no one else has.”

Sehgal also prefers tokens to biometrics, but says BMC is moving away from tokens because of their expense. The organization has begun using “push” technology, in which users specify how they want to be notified to verify their identities. For example, he says, “You could use an app on the phone that prompts you, saying someone who claims to be you is trying to log into the system. You could also be texted or called.”

The problem with biometrics, he adds, is that they’re costly to scale up and use in the long term. “The devices aren’t cheap, and the systems integration piece is limited.” Also, they can’t be used at home. He dismisses the idea of employing smartphones, saying their fingerprint scanners are not yet adequate for enterprise use.

Tokens are fine for accessing a network from home, Christly notes. In fact, they’re often applied first to enable remote users to access an enterprise system via a virtual private network. In contrast, he says, it’s “expensive and problematic” to provide card readers for every clinician at home.

AWARENESS GROWS

The healthcare industry is becoming more aware of the need for strong authentication, Wyrick says. In part, he notes, this is because of government regulations that require two-factor authentication for Electronic Prescriptions for Controlled Substances (EPCS). Meanwhile, to better protect patient privacy and security, a HIMSS Identity Management Task Force, recently recommended that patients undergo an identity proofing process and be issued a two-factor authentication credential before they access medical records on patient portals.

As a result of these developments and the growing problem of security breaches, more and more healthcare organizations are starting to look at the pros and cons of two-factor authentication. But the burden of strong authentication for access to different systems across the healthcare ecosystem remains a challenge.
“Strong authentication has historically been restrictive, it has required behavior change, and it’s been slow,” Wyrick acknowledges. “But it’s been secure. And more and more, we see the demand for convenience. How do we take what we’ve learned over the past 20 years and apply it today to an approach that’s convenient and secure? That’s where we’re heading.”

**DIGITAL IDENTITY MANAGEMENT**

Recently, a new approach to authentication has emerged. Known as “digital identity management”, this method of identity proofing individuals is based on the concept of an “identity ecosystem” that crosses business boundaries. Consonant with the growing emphasis on interoperability in healthcare and the push to improve care coordination, digital identity management holds the promise of simplifying access to disparate information networks while increasing the security of those networks.

Two-factor authentication is essential to this approach, because it provides assurance to entities within the identity ecosystem that the individuals seeking access to data are who they say they are. Conversely, digital identities could reduce the workflow burden of strong authentication by standardizing authentication across identity ecosystems.

The National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative, has been leading efforts to develop and promote secure, trusted digital identities. Secure and trusted access to electronic health records is a key initiative and is referenced throughout NSTIC documents. The private sector arm of this initiative is the Identity Ecosystem Steering Group (IDESG), which includes stakeholders ranging from regulated industries and IT infrastructure developers to consumer advocates, educational organizations, and civil liberties groups. Originally funded by NSTIC, IDESG has received financial support from the National Institute of Standards and Technology (NIST) since 2014. NSTIC defines an identity ecosystem as “an online environment where individuals and organizations are able to trust each other because they follow agreed-upon standards to obtain and authenticate their digital identities—and the digital identities of devices.”

“Trustmark schemes” that determine service provider compliance with the identity ecosystem framework. In healthcare, an identity ecosystem might include all of the healthcare entities that need to authenticate clinicians in order to grant them access to their information systems. For patients, the identity ecosystem might be designed to standardize authentication on all of their providers’ patient portals so they can view and download their medical records.
While it would be logical for identity ecosystems to begin as local or regional authentication networks, Christly raises the idea of developing a national digital identifier that would enable healthcare organizations to authenticate every person anywhere in the country. “If it comes from a national framework, there’s no reason why everybody across the country could not adopt that same process to identify that person,” he says.

CURRENT EXPERIMENTS

Digital identity management has been used in banking and is being tried in some other industries, including healthcare. Kaiser Permanente, Aetna and UnitedHealth are all participating in the IDESG, and seven of the 14 pilots funded by grants from NIST are in healthcare. For example, Inova Health Systems in Virginia has enabled 1,500 patients to securely obtain their personal health records by leveraging their authentication with Virginia’s Department of Motor Vehicles. Santangelo is very enthusiastic about the potential of digital identities in healthcare. Noting that population health management requires access to many systems across multiple provider entities, he says, “To maintain access to data in all of those environments is very complex. Having a centralized, secure identity management environment that you could use to navigate to all these various points of entry that are required to deliver population health and create an interoperable healthcare environment is an idea whose time has come.”

Christly, similarly, calls digital identity management “a great idea.” He especially likes the wide range of two-factor authentication methods that could be used. “If the core identity of that person is established well enough through this system, it would be great,” he declares. “If it could be used by either the patient or the provider and could be plugged into an SSO front end, it’ll work fine.”

Sehgal also sees potential benefits in secure digital identities, but cautions that it might take much more work to implement than anticipated, “because of the stale data that already exists. That’s the number one problem for a lot of identity programs: there are four to six ‘sources of truth’ for the average person, there’s a 25%-35% data inaccuracy rate, and the process to resolve those inaccuracies is usually manual,” he says. “When you’re talking about thousands of records that go back 15-20 years, a lot of organizations don’t want to deal with that.”

Nevertheless, he concedes that the digital identity management concept offers some security advantages. “If done right, digital identities will be able to tell you the attributes of the person and what is the relevance of that connection to the data that’s being sought at that time. Because it’s on a platform that’s highly scalable and automated, that process of identifying who they are, where they’re coming from, and why they’re connecting, and determining the risk can be made in close to real time.”

That’s the number one problem for a lot of identity programs: there are four to six ‘sources of truth’ for the average person, there’s a 25%-35% data inaccuracy rate, and the process to resolve those inaccuracies is usually manual.
PATIENT AUTHENTICATION

According to NSTIC, digital identity management in an identity ecosystem can:

• Enable patients to use a single trusted credential to log onto an EHR in the cloud
• Secure patient access to health information
• Streamline provider and patient access to multiple systems, including via Blue Button
• Improve the quality of care via the secure exchange of EHR data
• Reduce patient identity matching problems while protecting privacy.

The ability of patients to access their own records has been impeded by the need for them to view information from different providers on separate portals, unless their providers work for the same organization. The use of secure digital identities would not eliminate that barrier, but would make it easier for patients to see their records because they’d need only one set of credentials to access them on multiple sites. Of course, that assumes that all of their providers participated in an identity ecosystem.

Several methods have been used to help patients assemble their electronic records in one place, including the Blue Button technology. Blue Button was first introduced in the Veterans Affairs (VA) health system and later spread to Medicare and some private payers. The latest iteration of this tool, known as Blue Button Plus, aims to improve the security and privacy of patient access to EHRs. The Office of the National Coordinator of Health IT (ONC) is working with NSTIC on the authentication piece of this solution.

Health record banks—community organizations that put the patient in charge of all their personal health information—is another concept being considered. Under this approach, when care is sought, the patient gives permission for their healthcare professionals to access some or all of their up-to-date health records via a secure connection. When the care is complete, the new records from that visit are securely deposited in the health record bank—and made available for the future.
Meanwhile, the HIMSS Identity Management Task Force, in a document entitled “Recommended Identity Assurance for Patient Portals,” has recommended that all patients meet a “high confidence identity proofing standard” before being allowed electronic access to PHI. This high-confidence standard, the task force states, includes a combination of identity proofing and the use of two-factor authentication. “We believe that raising the confidence level of patient authentication now is important to counteract the rising security risk of using passwords alone,” the paper adds. While the HIMSS task force does not mention digital identity management, there are clear advantages to using strong authentications in this context. Besides facilitating access to records on patient portals, it would also help authenticate patients using mobile devices.

Santangelo views secure digital identities as a way to increase patient engagement. “Medical records belong to patients now, not the other way around. They also need to access and share that information with multiple systems because they’ve recognized themselves as the owners of that information.”

Christly believes that the digital identity management approach could help squelch consumer fraud, which is encouraged by the sharing of passwords. “When reviewing patient privacy audit logs, it can be hard to identify the person who looked at the patient’s record. I don’t know if it’s that person whose username appears in the audit trail, or if they shared their username and password with someone. This proposal would help verify that this person is who they’re supposed to be much better than we can do today.”

CLINICIAN AUTHENTICATION

The ability to recognize the digital identities of clinicians across care settings would facilitate their access to EHRs and other types of systems. “We want to avoid needing to have so many authentication methods and tools for different applications, which creates a barrier to these people doing their jobs,” says Wyrick.

A Utah hospital that uses VASCO’s two-factor identity-proofing method, he says, will soon start moving from point-to-point authentication to “continuous authentication.” A user will be authenticated to a workstation based on proximity and will then use single sign on to access a range of systems on that computer. Clinicians will be authenticated via Bluetooth devices attached to security badges as they move around the facility.

“It will give them access quickly to all the systems they need and in a clean way, because contamination and hands free are such big issues,” Wyrick points out.

“When reviewing patient privacy audit logs, it can be hard to identify the person who looked at the patient’s record. I don’t know if it’s that person whose username appears in the audit trail, or if they shared their username and password with someone.”

—John Christly
Digital identity management is the next step, he says. “SSO could be central to work in the hospital, but as you’re e-prescribing on a tablet, that’s something else [in security terms]. If you’re logging onto the EHR from home, that’s something else. So the challenge is finding a way to authenticate the person one time and use that, whether it’s through SSO or on their tablet or from home. That’s the missing piece.”

To Santangelo, the missing piece is simplicity. “Digital identity management presents an opportunity to centralize and secure authentication and allow a mobility and ease of use that’s needed,” he says. “If it’s too complex, people just aren’t going to use it. You’ve got to have a model that’s secure, but it’s also got to be easy to use and not overly complex. Otherwise, the users will find ways to circumvent it, and that’s where the security issues arise.”

**EPCS PAVES THE WAY**

Under the rules of the Drug Enforcement Administration (DEA), physicians and other clinicians who wish to electronically prescribe controlled substances must be identity-proofed by a DEA credential service provider or, in some cases, by their institution’s credentialing office. Prescribers must use two-factor authentication every time they prescribe a controlled substance.14

Wyrick has seen some New York doctors being authenticated differently for EPCS in various healthcare organizations. As more physicians go through this process, and have five or six different authentication methods in different places, he forecasts, “it will be frustrating for them.”

Digital identity management is not currently on the agenda for EPCS, Wyrick admits. But after physicians start using tokens or other two-factor authentication methods for EPCS, he argues, they can be persuaded to use it for other purposes, paving the way for digital identity management.

The Office of the National Coordinator for Health IT (ONC) has recommended that health care industry stakeholders begin leveraging the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guide for identity management standards and best practices. In addition, ONC has set a goal of at least 50% of health care organizations implementing identity proofing and authentication best practices by 2020.15

Technology vendors are starting to get the message about two-factor. Cerner, for example, has had DEA certification for three years, notes Chandra Venkat, business developer for integrated systems at Cerner. So its EHR has the ability to recognize two-factor authentication.
HEALTH INFORMATION EXCHANGE

Clinicians could also use their digital identities to log into a health information exchange (HIE), Christly notes. “Say you’re a doctor practicing at one hospital system, and you want to get into an HIE to view data put there by another hospital system. Do they both accept the same digital identity? If they do, that reduces the login stress and time to get to that crucial information for the doctor.”

Santangelo counters that information sharing in HIEs is between systems, not end users. But providers who work in multiple facilities could more easily get the information they need from those hospitals if they participated in an identity ecosystem, he notes.

“If there were a standardized way to authenticate, it just makes the navigation of all those systems easier for the end user,” he says. “And by making it easier, they’re going to use it, as opposed to finding alternative ways to gain access.”

UPGRADING OLDER SYSTEMS

Digital identity management proponents say it could improve the accuracy of patient matching in HIEs, accountable care organizations and other entities that aggregate patient data. Sehgal agrees that patient matching could be better if you didn’t have to spell a patient’s name right to identify that person uniquely. But every organization in an identity ecosystem would have to ensure that their systems could accept that digital identity. “It’s not that easily done, because the systems are old,” he points out. “The average EHR is 5-10 years old at this point.”

Would it be possible to persuade EHR vendors to equip their next versions with the ability to recognize these digital identities and to retrofit the older systems?

“It would be possible,” Sehgal replies. “But what’s the financial incentive for them? EHR vendors are for profit, and unless they see a gain, they’re not going to do it.”

Venkat, however, says that Cerner would outfit its products to accept digital identity management if its customers asked for it. “There are so many digital identities around, and being able to incorporate that into an identity ecosystem is pretty important,” he notes.

Cerner has architected its EHR to use open standards like the OAuth standard for authentication, so he expects the company would be able to adopt standards designed for an identity ecosystem, he continues.

“When we build our systems internally, we try to keep them as open as possible, using existing standards. That way, if something new comes up, we can use those standards to implement it rather than having to redo everything internally.”

“If there were a standardized way to authenticate, it just makes the navigation of all those systems easier for the end user. And by making it easier, they’re going to use it, as opposed to finding alternative ways to gain access.”

—John Santangelo
How about retrofitting older systems? If they were not originally built to meet modern security standards, Venkat says, Cerner could upgrade them by rewriting some components. “Our system provides a layered architecture, so we are able to replace some of the parts to be able to support the standards as they evolve.”

**READY FOR CHANGE**

Venkat believes that healthcare providers and EHR vendors are both ready for the advent of an identity ecosystem and digital identity management. “In my discussions with hospitals and other vendors, I see there’s an urgent need to integrate those systems beyond their own EHR infrastructure,” he observes. “I’m seeing a larger eagerness of the industry to move towards that than in the past.”

The new emphasis on interoperability requires a new approach to data security and authentication, he adds. “The interoperability goes hand in hand with the security aspect of the data that you’re sharing.”

Regarding his own company’s position on digital identity management, Venkat notes, “Cerner has always looked beyond the EHR as part of population health. Now we’re seeing clients wanting to do that, and that will help drive us toward digital identity management.”

“The interoperability goes hand in hand with the security aspect of the data that you’re sharing.”

—Chandra Venkat
CONCLUSION

The healthcare industry relies on an outdated framework for authenticating providers and consumers who want to access healthcare records. Usernames and passwords provide inadequate security for protected health information. They also pose a barrier to those who must remember a number of different logins and passwords to access various systems.

To solve this problem, more healthcare organizations must identity-proof those who seek access to their systems and implement two-factor authentication. The two-factor requirement for EPCS has provided a jolt of energy for organizations that want to move in this direction. But perceived issues of cost, complexity and convenience must still be addressed.

Once identity proofing and strong authentication become widespread, secure, trusted digital identities can be used to increase security and convenience. By giving healthcare providers and staff members unique digital identities that they can use across an identity ecosystem, digital identity management will increase security while lowering the workflow burden of two-factor authentication. Including patients in the identity ecosystem, coupled with strong authentication, will better protect the privacy of their health information and will facilitate their ability to view their records on multiple patient portals.

It will take some time for a private-public consortium to sort through the issues of the identity ecosystem and formulate standards for leveraging it in healthcare. Until then, healthcare organizations should become aware of this approach and ask their EHR vendors to integrate digital identity management into their products when it is ready for adoption.
RECOMMENDATIONS

Adopt two-factor authentication across the healthcare organization.

Centralize authentication within the enterprise information system, perhaps by using active directory function.

Combine strong authentication with single sign on to provide secure access while lowering the burden on workflow.

For second factors of authentication, choose the methods that work best for your providers and staff within your organization’s environment.

Consider using two-factor authentication of patients on patient portals when your EHR vendor upgrades its portal software for that.

Ask your EHR vendors whether their systems are capable of handling digital identity management.

Be ready to use digital identity management when it becomes available.
REFERENCES


2. Wikipedia, LDAP.


8. Ibid.


10. Ibid.

11. Ibid.


13. “Recommended Identity Assurance for Patient Portals”
