White paper

The Evolution of the Digital Identity in Healthcare

VASCO®
THE AUTHENTICATION COMPANY

Table of Contents

Introduction	4
Regulations and Cyber Risk	5
Critical Tools for Enabling Digital Identities and Identity Access Management	9
Factors to Consider When Evaluating Security and IAM Vendors	11
Preparing for a Digital Future	13
Research Sources	14

Introduction

The healthcare industry, not unlike the banking, manufacturing and retail sectors, is in the middle of a massive digital transformation. In an effort to make healthcare delivery more efficient and effective everything from lab results and prescriptions to patient health records is moving to an electronic state.

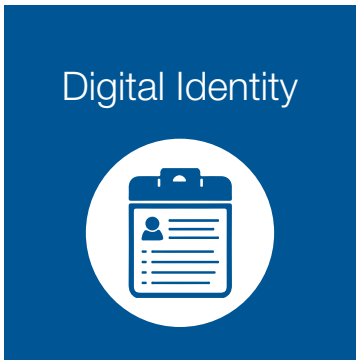
For providers and vendors alike, the proliferation of internal and patient-facing technology requires a shift in thinking, primarily in regard to user identities. It's no longer enough to simply know which users have access to an organization's healthcare IT systems; all users, providers, administrative staff and patients, must be equipped with secure, trusted identities.

But while some institutions are starting to embrace sophisticated biometric and near field communication tools to verify identities, most organizations lag behind.1 Many providers still rely on simple, unsecure usernames and passwords for employees to access critical data systems and sensitive, legally protected information — a risky practice that leaves providers, vendors and patient data susceptible to breaches and privacy concerns.

Prompted by new regulatory requirements and a rapidly evolving technology climate, the healthcare industry is moving towards a future where patient and operational data can be digitally communicated in a secure way. Reaching this future state requires organizations to develop and support an ecosystem of digital identities, which hinges on three essential components: identity proofing, authentication and authorization.

Now, the onus falls on healthcare providers to adopt (and healthcare IT vendors to deliver) secure yet convenient solutions that enable compliance with tightening federal laws, improve security and accessibility, and pave the way for interoperability throughout the industry.

Regulations and Cyber Risk: Fueling the Movement Toward Digital Identities



Over the last few years, a combination of increased government regulation and an intensifying cybersecurity landscape has powered the healthcare industry's shift to digital identities.

The HITECH Act and EHR Meaningful Use

In 2009, the federal government signed the Health Information Technology for Economic and Clinical Health (HITECH) Act into law, giving the U.S. Department of Health & Human Services the power to develop programs to improve healthcare outcomes through technology.[2] This legislation led to one of the most prominent government-sponsored healthcare IT initiatives to date, the Centers for Medicare & Medicaid Services' EHR Incentive Programs.

Through these programs, U.S. healthcare providers are encouraged to implement and demonstrate meaningful use of electronic health record technology. The CMS outlines three stages that eligible professional and hospitals must complete in order to achieve "Meaningful Use", with specific objectives focused on protecting patient health data and improving care, transparency and efficiency. Failure to comply results in financial penalties via Medicare Reimbursements [3]

The initiative's Stage 1 and 2 meaningful use objectives require healthcare providers and practitioners to accommodate e-prescribing (eRx) and sufficiently protect patients' electronic health information. Stage 2 is focused on information exchange and care coordination. A key Stage 2 requirement is providing patients the ability to view online, download and transmit their health information. This is commonly referred to as the "VDT" and must be done within four business days of the information being available to the eligible provider (EP) and within 36 hours after discharge from the hospital. Stage 2 also places an emphasis on health information exchange between providers to improve care coordination. One of the core objectives for both EPs and eligible hospitals and CAHs requires providers who transition or refer a patient to another setting of care or provider of care to provide a summary of care record for more than 50% of those transitions of care and referrals.

By providing patients the ability to view online, download and transmit their health information it is imperative that there is a high level of assurance that it is really the patient (or proxy) accessing the sensitive data. Without proper safeguards in place, this patient engagement requirement can open the doors for identity thieves and put organizations at risk for breaches.

All providers will be required to comply with Stage 3 requirements beginning in 2018 using EHR technology certified to the 2015 Edition. Stage 3 adds a host of requirements. Most applicable to this white paper is the addition of the VDT requirement in Stage 2 to include patient access their health information through an API. It is important to note, that CMS does not require a "patient portal" for VDT, and they do not limit innovation in software or systems used to allow patients to access and engage with their health information.

Additionally, safeguarding electronic protected health information (ePHI) is essential to all aspects of meaningfully using EHRs, as the consumer must have trust in the integrity of the security of their personally identifiable information to engage in the use of health IT.

Eligible providers, eligible hospital, or critical access hospital (CAH) must do the following to comply [4]

- Conduct or review a security risk analysis in accordance with the requirements of 45 CFR 164.308(a)(1) of the HIPAA Security Rule. The security of ePHI created or maintained by the CEHRT must be addressed (including encryption).
- Encryption is an addressable implementation specification of the HIPAA Security Rule (45 CFR 164.312(a)(2)(iv)).
- General rules regarding addressable implementation specifications are set forth at 45 CFR 164.306(d)(3).
- Implement security updates as necessary as part of the risk management process.
- Correct identified security deficiencies as part of the risk management process

Although two-factor authentication is not required, it should be noted that having only a password, is considered deficient in terms of meeting compliance with many of the HIPAA Security Rule subparts contained within

- 164.308 – Administrative safeguards
- 164.310 - Physical safeguards
- 164.312 – Technical safeguards
- 164.314 – Organization requirements

EPCS Compliance

Another factor fueling the need for secure healthcare digital identities is Electronic Prescriptions for Controlled Substance (EPCS). In March 2010, The U.S. Drug Enforcement Administration published its Final Rule. The rule spells out specific requirements for providers that electronically prescribe controlled substances, and pharmacists who dispense controlled substances and the technology that is used for e-prescribing activities.

The regulations provide pharmacies, hospitals, and practitioners with the ability to use certified electronic prescribing software for controlled substance prescriptions while maintaining

the closed system of controls on controlled substances dispensing.

Although the DEA established the rules for EPCS, legalizing it is up to each individual state. As of 2016, All 50 states have legalized EPCS for Schedule II-V controlled substances.

EPCS offers significant efficiencies to all parties.

- Obviously paperwork is reduced, but more importantly EPCS significantly reduces prescription forgery.
- EPCS also reduces the number of prescription errors caused by illegible handwriting and misunderstood oral prescriptions. Phone calls to and from the provider and the pharmacist have been reduced.[5]
- Patients no longer have to worry about lost or misplaced prescriptions and drug adherence rates have increased with ePrescribing.

Though electronic prescriptions aren't mandatory, providers that prescribe controlled substances electronically must have proper identity proofing and two-factor authentication mechanisms in place to stay compliant. Under EPCS, individual practitioners need to apply for authentication credentials through government-approved credential service providers or certification authorities, which oversee an identity proofing process that adheres to the National Institute of Standards and Technology's Special Publication 800-63-1 Assurance Level 3.

When electronically signing a controlled substance prescription, providers must provide two factors for authentication (a combination of something the user knows such as a password or PIN, something the user has, such as a hardware token or software token installed on a mobile device, or something the user is, a biometric). Hardware tokens are required to be cryptographic devices that meet the Federal Information Processing Standard (FIPS) 140-2 Security Level 1.[6] at a minimum. NIST defines Security Level 1 as appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent.

Realizing healthcare security is not "low-level security", healthcare organizations addressed this concern by proactively equipping providers with 140-2 Security Level 2 compliant devices. Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module.

Surescripts Identity Proofing Requirements

Leveraging the identity proofing requirements defined by the DEA and NIST, Surescripts has instituted its own identity proofing requirements for all prescriber participants connecting to the Surescripts network for ePrescribing transactions. These requirements went into effect on April 27, 2016 and apply only to non-controlled substances. EHR vendors failing to comply risk their ePrescribing software becoming decertified by Surescripts.

Directed Exchange - "Direct"

In May 2013, HHS's Office of the National Coordinator for Health IT (ONC) published messaging guidelines to the Direct Applicability Statement (ONC Direct Guidelines to Assured Security and Interoperability) that recommended provider Direct email addresses only be issued to individuals and organizations that have been identity proofed to NIST LoA 3 or higher. The guidelines also recommended that the equivalent of NIST LoA 3, and that Federal Bridge Certificate Authority (FBCA) cross-certified certificates (or their equivalence), should be utilized.

Healthcare's Cyber Risk Challenges

The impetus behind these regulations and authentication controls — beyond the need to modernize healthcare operations — is to protect organizations and patients from growing cybersecurity threats.

As of August 2015, the medical and healthcare industries accounted for 36 percent of the country's data breaches year-to-date, consisting of 167 breaches and nearly 110 million exposed records.[7]

These incidents inflict significant reputational and financial damage on affected providers, costing the healthcare industry billions. According to Ponemon Institute research, the average cost of a breach for organizations is more than $3.8 million, a jump of 23 percent from 2013. [8]

More than 90 percent of surveyed organizations have endured a breach, and 65 percent cited electronic-based incidents occurring in the last two years. Malicious third-party actors, however, are not the leading cause of these events. Almost three-quarters of healthcare organizations rank employee negligence as the top security threat to their operations.[9]

The financial impact of a breach is not the only adversity plaguing breached healthcare organizations. The public relations impact can be even more damaging. In addition to being front page news, a permanent posting on HHS's " Wall of Shame", the list of breaches of unsecured protected health information affecting 500 or more individuals. as required by the HITECH Act be equally damaging.

In a digital-first world, the threat landscape can change in an instant. The healthcare industry's technological shift is inevitable; providers and vendors need the security mechanisms in place to navigate this evolution strategically and protect patients in the process.

Critical Tools for Enabling Digital Identities and Identity Access Management

Wedged between strict regulatory guidelines and extraordinarily sensitive client information, healthcare organizations can't afford to take any chances with data security. According to Ponemon Institute research, however, only a third of healthcare organizations feel that they have the resources to prevent or detect unauthorized patient data access or loss, including theft.[10] Firms need to have the right tools to keep their data safe, authenticate end-users, and maintain manageable IT environments.

Fortunately, there are a number of available solutions that align with each of these needs:

- **Identity proofing services:** In response to more stringent compliance standards, a market has emerged for certified, automated identity proofing that adds a layer of IT security without complicating system or device management. Through these services, third-party proofing providers collect a variety of users' personal details (including their name, date of birth, Social Security number and address), validate this information, and grant requisite certificates. Vendor proofing solutions can be invaluable for larger organizations that need to certify high volumes of user identities at once, across geographically diverse locations.

- **Two-factor authentication:** A number of security providers now offer physical tokens, smart cards and other devices that generate one-time unique passwords to satisfy the “something you have” two-factor authentication criterion for user verification. Increasingly, vendors are developing biometric authentication solutions to fulfill the “something you are” factor as well. Fingerprint readers comprise most of the biometric tools available today, but advances in voice recognition and retinal scanning technology may steadily push these options into mainstream enterprise use.

- **Authentication servers**: Centralized, server-side verification is essential for healthcare organizations supporting a variety of authentication methods. Authentication servers provide the flexibility to verify access requests regardless of origin, from virtual private networks (VPNs) to web and cloud-based applications. If implemented improperly, authentication servers can represent a single point of failure and a prime target for malicious actors, so it’s imperative that healthcare organizations seek out established vendors with proven security track records.

Factors to Consider When Evaluating Security and IAM Vendors

Recognizing the need for an Identity Access Management (IAM) solution is only half the battle; choosing the right vendor can be an equally strategic, selective process.

Identity management is far from unique to the healthcare field; sectors as diverse as retail and banking are scrambling to adopt comprehensive identity verification and authentication solutions. With nearly limitless IT security vendors to choose from, assessing a provider's industry familiarity is often as important as assessing their products. Sector-specific identity proofing and authentication challenges mean that healthcare organizations need their solution providers to act as partners, not merely vendors.

Given healthcare organizations' high stakes regulatory needs, it's also essential to look for providers with relevant certifications (or certified products). Just because a digital security vendor offers multi-factor remote network authentication solutions does not automatically mean those products adhere to NIST Special Publication 800-63 Assurance Level 3 standards. And while many tools accommodate role-based authentication, few offer the physical tamper evidence required for FIPS 140-Level 2 certification.

Similar to a vendor's industry expertise, it's important to consider how its solutions will integrate with your organization's existing IT environment. An IAM tool without native integration capabilities can quickly create headaches for firms that must bridge the gaps themselves. This not only represents an additional expense, but also a source of risk. Any oversights in the handoff between disparate systems could result in security vulnerabilities and even data breaches. For healthcare organizations integrating a variety of record systems, a DIY solution is usually out of the question.

At the same time, healthcare organizations should carefully understand any potential risk that may be inherited through their vendor. Reputable vendors should be transparent regarding their data breach notification policies, including clearly defined obligations and clients' recourse if sensitive information is jeopardized. Due to the sensitive nature of patient data, healthcare providers and vendors need partners that will be proactive and responsive during a crisis.

VASCO Healthcare Solutions for Providers and Vendors

As a global leader in protecting the world's most sensitive information, VASCO offers a variety of authentication and digital identity protection solutions to help healthcare organizations solve their IT security and compliance needs:

Identity Proofing: VASCO's solution safely and conveniently provide remote identity proofing for electronic prescribing, in compliance with the DEA's ECPS mandate. This solution meets NIST Special Publication 800-63 Assurance Level 3 requirements for multi-factor remote network authentication, allowing organizations to focus more on patient service than regulatory red tape.

Authentication Modalities:

- Hardware one-button token
- FIPS140-2 Compliant
- EPCS Compliant
- Can be used across PC and mobile
- Mobile token
- FIPS Compliant*
- Mobile Push
- Secure Communication Channel

Back-end Infrastructure

- Native integrations with existing EHR/ERX applications
- EHR specific plug-ins
- IDENTIKEY Authentication Software Server
- VACMAN Controller API

(*) Certification in progress

Preparing for a Digital Future

The healthcare sector is rapidly changing, and organizations across the industry have no choice but to adapt. Due to regulatory measures, evolving risks and a push to root out inefficiency, healthcare providers and vendors face pressure to innovate around data security. Not surprisingly, this has elevated technology beyond the IT department's purview to the center of all healthcare operations.

The next stage of the healthcare industry's transformation requires organizations to safely and conveniently communicate electronically, removing bottlenecks from the information exchange process without sacrificing convenient access to patient records.

Firms need comprehensive digital strategies that include identity proofing, authorization and authentication measures, but they can't achieve this without third-party support. Practitioners, hospitals, labs and pharmacies need to partner with vendors that consider all possible impacts within the context of the healthcare sector, providing certified systems that seamlessly integrate with other tools, safeguard patient data and simplify user workflows.

In many instances, healthcare organizations have become accustomed to simple usernames and passwords, fragmented applications and manual recordkeeping – making the vision of a digital, interoperable future even more jarring. But with the right tools and the right partners, the drive to meet these operational and regulatory challenges will leave organizations not only safer, but more agile than ever before.

Research Sources

(1) "How biometric palm scans help keep hospitals secure," Augenbraun, Eliene. CBS News. October 27, 2014. www.cbsnews.com/news/patientsecure-biometric-palm-scan-system-hospital-security

(2) "HITECH Act Enforcement Interim Final Rule," U.S. Department of Health & Human Services. www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

(3) www.healthit.gov/providers-professionals/faqs/are-there-penalties-providers-who-don%E2%80%99t-switch-electronic-health-record

(4) www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications

(5) healthitinteroperability.com/news/medication-data-in-ehr-provides-basis-for-tracking-adherence

(6) "Electronic Prescriptions for Controlled Substances (EPCS): Interim Final Rule and Request for Comment Questions and Answers for Prescribing Practitioners," U.S. Department of Justice, Drug Enforcement Administration. March 31, 2010. www.deadiversion.usdoj.gov/ecomm/e_rx/faq/practitioners.htm

(7) "Data Breach Reports," Identity Theft Resource Center. August 11, 2015. www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

(8) 2015 Cost of Data Breach Study: Global Analysis, May 2015) www.fiercehealthit.com/story/data-breach-costs-rise-23-percent-2013/2015-05-28

(9) "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data," Ponemon Institute LLC. May 2015. www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data

(10) Ibid.

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com