One User, One Device

How Trusted Digital Identity Reduces Multiple Passwords While Protecting PHI

VASCO®

Table of Contents

All other trademarks or trade names are the property of their respective owners. Any trademark that is not owned by Vasco that appears in the document is only used to easily refer to applications that can be secured with authentication solutions such as the ones discussed in the document. Appearance of these trademarks in no way is intended to suggest any association between these trademarks and any Vasco product or any endorsement of any Vasco product by these trademarks' proprietors. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.

Introduction

The average clinician spends 122 hours a year (the equivalent of three average work weeks) trying to access various forms of electronic medical records (EMR) [(1)], That time — which could otherwise be spent on direct patient care — results from the overabundance of passwords and logins required to access the applications needed for accessing patient records.

Then there are federal mandates such as the DEA EPCS (E-Prescribing of Controlled Substances) to ensure EPCS compliance for prescribers and the Health Insurance Portability and Accountability Act (HIPAA) that establishes national standards to protect individuals' electronic protected health information that is created, received, used, or maintained by a covered entity.

With the massive push towards electronic health records management and compliance of healthcare providers with federal mandates, there is a clear need to establish digital trust in healthcare[(2)]. The U.S. Department of Health & Human Services is driving "Verifiable Identity and Authentication of All Participants" with the 2015-2017 goal of 65% of health care organizations enabling patient access to patient portals with support of knowledge-based attributes or emerging authentication technologies in lieu of passwords to reduce vulnerabilities to identity theft [(3)].

Why Single Sign-On (SSO) Demands Stronger Authentication

Q. What is Single Sign-On?

A.

- Single Sign-On (SSO) is a session and user authentication service that permits a user to authenticate once with existing credentials in order to access multiple resources.

Q: What are the types of SSO solutions currently in use by the healthcare industry?

A:

- The first type injects the user's credentials into health applications after the user has logged into Windows. In this instance the user's credentials for the different applications might be different. This is hidden for the user by the SSO solution.
- The second relies on the fact that EHR applications are increasingly integrated with Microsoft Active Directory. As a result, the same credentials can be used to log onto multiple health IT applications. By implementing two-factor authentication (2FA) in Active Directory, health IT applications can immediately benefit from 2FA.

  Note: While the first type is the predominant Single Sign-On solution for providers, it has several disadvantages including additional and increased difficulty in integrating 2FA. As a result, the second type, at least when it comes to two-factor authentication, becomes the preferred version to supplement and strengthen SSO.

Most healthcare organizations are firmly focused on security and compliance and today most leverage Single Sign-On (SSO) as a way to federate identity in healthcare settings (e.g. the ability for a user to be able to access all of the resources they need by authenticating to a system once without needing to re-authenticate for subsequent access to those same resources).

However, to deliver optimal patient care they must also address the integration and management challenges inherent in integrated EHR. A delivery system that includes two-factor authentication which provides simultaneous, secure, and convenient access to patient applications, safeguards a provider's most important assets — protected health information (PHI) and public trust.

As a result, safeguarding this exchange of information demands trust. Trust in users, platforms, applications and devices. As this Solution Brief suggests, it also demands a holistic, integrated and end-to-end ecosystem built on trusted digital identities that helps healthcare organizations to make a shift from securing individual unconnected pieces to delivering a complete security solution based on trust that allows patients to do more, with greater convenience and productivity.

Q. What are the advantages of Single Sign-On?
A.

- The user can authenticate during their first access to an application, and subsequently be given automated login to any additional applications they access after that initial login. Depending upon the technology in place, the Single-Sign-On process typically involves the concept of a "session", whereby the initial login is deemed sufficient for an administratively configured amount of time, after which the user may be asked to be authenticated again in order to establish another valid session.

Q: What are the some of the key concerns associated with Single Sign-On?
A:

- SSO is great for convenience, but done poorly, SSO can actually make environments less secure and more susceptible to breaches. With a single set of credentials protecting multiple resources, "all your [authentication] eggs are in one basket".
- With the importance of the user authentication process magnified, many times complex password rules when using SSO can make for a poor user experience (users forgetting passwords, password resets, passwords written down and potentially compromised)
- So, while SSO offers great advantage, it can potentially introduce greater risk. The best way to counter this risk is to implement multi-factor authentication as part of the SSO process.

Empowering Trust in Provider Settings

In the digital world trust is elusive, even as physicians have moved on from color-coded folders to document patient records to rely on Single Sign-On to access patient records.

Further, given the increasingly heterogeneous nature of medical systems including those storing electronic health records, a User ID and password that might 'work' for a given application may require a different authentication mechanism altogether for another. Over time these combinations of User IDs and passwords quickly become unwieldy, even untrustworthy, frustrating the physician trying to negotiate, manage and update EMRs while sufficiently managing his patient case load.

So, how do you define trust? Well, in the context of security and technology, trust is formed between:

- Users and Client Applications
- Client Applications and Server Applications
- Server Applications and Users

For any industry, healthcare included, achieving trust is not, at least initially, conferred only once. It occurs throughout the transaction chain:

1. **Identity proofing** (are you really who you say you are)
2. **Two-Factor authentication** (can the user you've presented be confirmed and validated through available authentication methods)
3. **Platform security** (is the platform [device and application] you are using to conduct the transaction known to be trusted)
4. **Transaction security** (is the exchange of data and the process used to exchange that data between you and a recipient trustworthy)
5. **Risk management** (is your online behavior, monitored throughout subsequent transactions, reliable and consistent or evasive and suspicious).

With trust established at each link in the chain the result is a secure digital platform that delivers much needed trust to the digital world: for patients, physicians and providers.

Protecting PHI Using Two-Factor Authentication

As we've seen, while Single Sign-On has been the "go-to" technology of choice for many providers, it can actually make environments less secure, less trustworthy and more susceptible to breaches. In fact, SSO is the epitome of a use case where one size simply does not fit all.

As a result, two-factor authentication[4] has emerged as a best practice for protected health information, requiring an additional form of identification beyond a username and password to access personal data.

Two-factor authentication is the process where two of the three possible factors of authentication are combined to authenticate the user attempting to gain access.

The possible factors of authentication are:

1. something the user knows – a password/PIN
2. something the user uniquely has – a key fob, their phone or an ATM card
3. something the user is – a biometric such as a fingerprint

In a healthcare setting, once the individual is verified through these means they are granted access to PHI including electronic health records and digital billing invoices.

An ONC (Office of the National Coordinator for Health Information Technology) brief (5) found that among non-federal acute care hospitals in the United States adoption of two-factor authentication has increased 53 percent in 2014 from the percent of hospitals who said the same in 2010. In fact, well over half of larger hospitals (63 percent) and medium-sized hospitals (59 percent) have two-factor authentication capabilities.

Significantly, HIPAA offers two-factor authentication as a possible method to provide security for PHI. In addition, two-factor authentication is an essential capability for providers who e-prescribe controlled substances. And although two-factor authentication is not currently 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

Healthcare's Cyber Risk Challenges

The emergence of two-factor authentication — beyond the need to modernize healthcare operations — is increasingly a necessity to protect organizations as well as patients from growing cybersecurity threats.

Based on its Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data [6], Ponemon estimates that data breaches could be costing the healthcare industry $6.2 billion.

Amongst its findings:

- Over the past two years the average cost of a data breach for healthcare organizations is estimated to be more than $2.2 million. The average cost of a data breach represented in its research is more than $1million.

- In spite of this, about half of all organizations have little to no confidence they can detect all patient data loss or theft.

- Keenly, eighty-nine percent of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past 24 months.

- Correlating data reveals that 50 percent of healthcare organizations report the root cause of a data breach was a criminal attack with 41 percent reporting it was caused by third-party error.

According to Reuters [7], medical information such as an electronic health record, is worth 10 times more than credit card numbers on the black market. In fact, stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number.

If hackers target your stored health information, including patient care and documents and the only thing protecting you is a simple Single Sign-on tool, it likely won't be enough to keep a hacker from obtaining your valuable personal data.

How VASCO Enables Trusted Digital Identities

VASCO solutions, including identity proofing and multi-factor authentication, enable healthcare providers and healthcare software vendors to rapidly implement two-factor authentication with improved compliance and greater efficiency.

Identity Proofing

Identity proofing is a critical requirement to establish a trusted digital identity and is a requirements of the DEA for EPCS Compliance (Electronic Prescribing of Controlled Substances). For security purposes, authentication credentials that are used to sign prescriptions can only be issued to practitioners whose identity has been confirmed and validated. Healthcare providers must offer to their prescribers both in-person and remote identity proofing that meets DEA and NIST Assurance Level 3. It is also the mandatory process for validating that a person is who he or she claims to be.

VASCO's MYDIGIPASS for Healthcare's identity proofing service streamlines the process of third-party confirmation of provider eligibility, and efficiently authenticates providers for the electronic prescription of controlled substances.

MYDIGIPASS for Healthcare[8] fulfills the NIST Special Publication 800-63 Assurance Level 3 requirements, and meet a critical EPCS compliance requirement. For security purposes, authentication credentials that are used to sign prescriptions can only be issued to practitioners whose identity has been confirmed and validated.

Among its features:

- Multi-application and platform versatility. MYDIGIPASS for Healthcare offers a single integrated and complimentary ID proofing method and authentication tool that can be used across all applications and platforms.

- A high level of trust on a single platform. MY DIGIPASS for Healthcare is an end-to-end identity proofing solution that facilitates secure information exchange between users and their applications throughout the organization. As a result, each user has a single, secure and trusted digital identity.

MYDIGIPASS for Healthcare is complete, compliant and reliable and is certified under the SAFE-BioPharma FICAM Trust Framework at NIST SP 800-63 Level of Assurance 3 as full-service Credential Service Provider as required by DEA.

FIPS 140-2, Level 2 Certified Two-factor Authentication

A convenient, single-button OTP (one-time password) authenticator, VASCO's DIGIPASS GO 7[9] provides a unique password each time the user remotely accesses a network, system or website. The DIGIPASS GO 7 FIPS 140-2 Level 2 token can be used across PC and mobile platforms, and satisfies two-factor authentication requirements for EPCS, Ohio's positive identification requirements for legend prescribing as well as EHR Stage 3 meaningful use.

Further, MYDIGIPASS for Healthcare supports trusted digital identities and secure information exchange through Remote Identity Proofing via Knowledge-Based Authentication (KBA) or live video session.

Multi-Application and Multi-Platform Security

MYDIGIPASS for Healthcare offers a unified ID proofing method and authentication tool that can be used throughout all applications and platforms. It also works ANYWHERE inside the healthcare facility or off-site, even when no cellular service is available. This critical flexibility is accomplished via the following products:

- **DIGIPASS GO 7**, a FIPS 140-2 Level 2 Certified one-time password hardware token
- **DIGIPASS for Mobile**[10], a DEA compliant software authentication tool that does not require cellular service to operate

Authentication Related Solutions

DIGIPASS as a Service — VASCO's flexible and cost-efficient solution includes a fully redundant hosted authentication back-end and the provisioning of DIGIPASS software or hardware authenticators to end-users. Because it is cloud-based, providers will not have to host the authentication in-house. This reduces capital and maintenance costs while enabling them to add strong authentication to their applications.

IDENTIKEY Authentication Server (IAS) — is a comprehensive, centralized and flexible authentication platform designed to deliver complete authentication lifecycle management via a single, integrated system. It offers secure and seamless access to corporate resources and applications of all kinds, from SSL VPNs to cloud-based apps and, through its integration with Active Directory, simplifies authentication management by serving as a single point of access for administrators and users alike. By adding a security layer to the logon procedure over the Internet, IAS secures remote users, offices, traveling staff and business partners.

From identity proofing and provisioning to secure login and fulfillment — all aspects of digital identity management are addressed on a single, fully integrated platform.

VASCO: The Trusted Platform for Healthcare Providers

The VASCO Trust Platform is a unique ecosystem built on trusted digital identities. We help healthcare organizations to make a shift from securing individual unconnected pieces to delivering a complete security solution based on trust that allows patients and providers alike to do more, with greater convenience and productivity.

Supplemented by two-factor authentication, end-to-end identity proofing facilitates secure information exchange between all access points throughout the healthcare ecosystem including:

- Patients logging onto an electronic portal
- Physicians reviewing a patient's health information using an EHR system
- Staff accessing the state's prescription drug monitoring program
- Physicians electronically prescribing medication for a patient's use
- Administrative staff submitting a claim to the payer
- Business Associates accessing patient data

The tight integration between Identity Proofing Services and Two-Factor Authentication coupled with Multi-Application, Multi-Platform Security ensures all transactions and data exchange are executed with the highest level of trust. In turn, this enables physicians, nursing staff, administrators and others to retain a single digital identity, regardless of the type of application, system or platform they use in their day-to-day responsibilities. Additionally, as we have established, two-factor authentication also strengthens Single Sign-On authentication for providers.

This singular, "One User, One Device" approach for healthcare providers will not only improve user experience — e.g., significantly reducing the number of logins and passwords required to access and annotate patient records, but also enable them to spend more time on patient management and care.

Sources

1. http://www.beckershospitalreview.com/healthcare-information-technology/ponemon-institute-inefficient-access-to-patient-information-costs-hospitals-2m-each-year.html
2. https://www.vasco.com/solutions/healthcare-information-security/index.html
3. https://www.healthit.gov/policy-researchers-implementers/interoperability
4. https://www.vasco.com/two-factor-authentication.html
5. http://dashboard.healthit.gov/evaluations/data-briefs/hospital-two-factor-authentication.php
6. http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1
7. http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
8. https://www.vasco.com/solutions/healthcare-information-security/mydigipass-for-healthcare.html
9. https://www.vasco.com/products/two-factor-authenticators/hardware/one-button/digipass-go-7.html
10. https://www.vasco.com/products/two-factor-authenticators/software/mobile/digipass-for-mobile.html

About VASCO

VASCO is a global leader in delivering trust and business productivity solutions to the digital market. VASCO develops next generation technologies that enable more than 10,000 customers in 100 countries in financial, enterprise, government, healthcare and other segments to achieve their digital agenda, deliver an enhanced customer experience and meet regulatory requirements. More than half of the top 100 global banks rely on VASCO solutions to protect their online, mobile, and ATM channels. VASCO's solutions combine to form a powerful trust platform that empower businesses by incorporating identity, fraud prevention, electronic signatures, mobile application protection and risk analysis.

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

THE AUTHENTICATION COMPANY