Using Trusted Digital Identities and Multi-Factor Authentication to Secure Patient Portals

VASCO

Table of Contents

Introduction

The electronic patient portal, a virtual yet highly-efficient channel for physicians and patients to exchange information, is rapidly emerging as a digital complement to the traditional office visit.

So, what exactly is a **Patient Portal**?

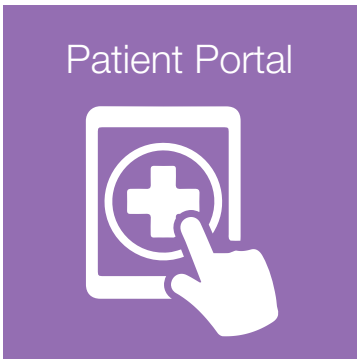
As defined by HealthIT.gov[1], a patient portal is a secure online website that gives patients convenient 24-hour access to personal health information from anywhere with an Internet connection where patients can view health information such as:

- Recent doctor visits
- Discharge summaries
- Medications
- Immunizations
- Allergies
- Lab results

Some patient portals also allow patients to:

- Exchange secure e-mail with their health care teams
- Request prescription refills
- Schedule non-urgent appointments
- Check benefits and coverage
- Update contact information
- Make payments
- Download and complete forms
- View educational materials

Among other outcomes, patient portals can increase patient engagement, customize care, enable patients to communicate with their providers on-demand and, potentially, to make positive changes in their behavior and lifestyle.



Once patients have registered for the portal they can access them via multiple channels: desktop, laptop, smart phones, tablets with varying operating systems — necessitating a way to credential and authenticate patients remotely.

Today, however, the overwhelming majority of patient portals are accessed via a username and static password. Unfortunately, static passwords are not secure, can be guessed, or hacked.

More problematically, what otherwise appears to be a routine, even turnkey exchange of Protected Health Information (PHI) between a patient (using a portal) and their provider presents risk, especially with PHI widely considered a highly valued commodity for resale by cybercriminals.

As a result, safeguarding this exchange of information demands trust. Trust in users, platforms, applications and devices. As this white paper suggests, it also demands a unique, holistic 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.

A Perceived Trade-off Between Convenience and Security

As is typical in healthcare, user convenience typically outweighs authentication and security best practices. The end result is that healthcare is the number one target of hackers due to the vast amount of Protected Health Information (PHI) contained in electronic health records and personal health records. Poor security puts patients' PHI at risk.

Since access to past records of care (including diagnoses, procedures, test results and prescriptions, among other facts) is critical to the provision of safe and effective healthcare, an accurate and unique **digital identity**[2] must be created for each patient such that it can be securely trusted across all those organizations over time to accurately link to past records of care. When implemented in ways that engender trust in the privacy and security of their records, this digital identity will also empower patients to securely navigate the healthcare system electronically and help manage their health activities while mitigating risk and arming themselves against fraud and cyber-hackers.

From the perspective of these digital identities, a patient typically has two types of interactions with a specific and usually local healthcare system; the first encounter (identity proofing) and all subsequent encounters (identity authentication). Although many organizations perform some identity proofing checks before granting access to a patient portal, they typically fall short when it comes to properly authenticating the patients each time they access the portal.

When patients access a patient portal today, they typically do so by using a User ID and static password combination for electronic authentication[3]. The process by which they initially obtain the User ID and static password, (i.e., the way they are proofed), typically involves them receiving a one-time code during an office visit (in-person identity proofing) or via paper mail. Some organizations also allow for online remote identity proofing by the asking of questions, the answers to which only the patient is expected to know (Knowledge Based Verification or KBV).

Given the onslaught of cyberattacks against healthcare coupled with the sensitive and HIPAA protected data stored in patient portals, providing the same level of authentication as purchasing movie tickets is a cause for concern for patients, healthcare organizations and providers. Moreover, since passwords are often shared or worse, stolen, there is no audit trail offering high confidence in who has accessed the portal.

Also, providers offering mobile app versions of the portal should harden the apps with bank-level security.

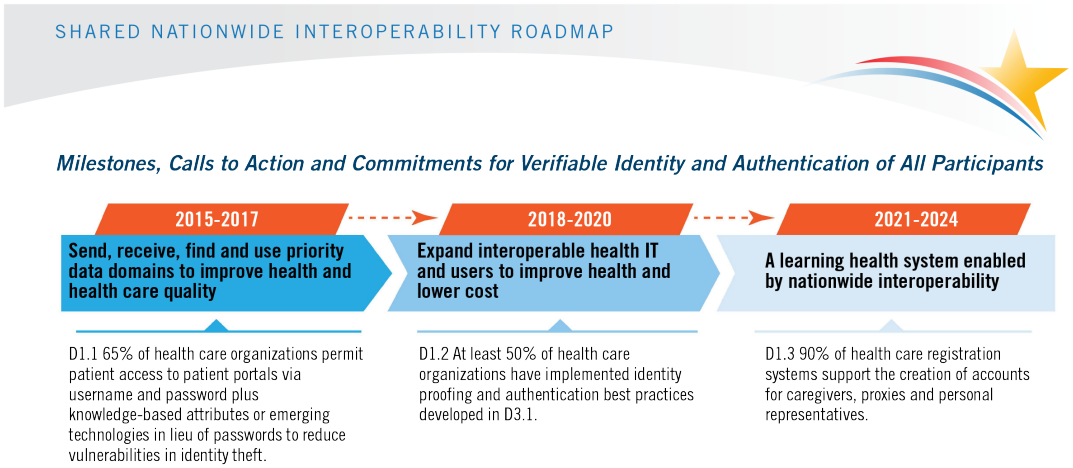
This is one of those classic cases where an organization has a very big problem and may not realize it. The focus on identity management and authentication as part of an overall strategy to enable a responsible healthcare cybersecurity strategy is proof positive that protecting PHI with a username and static password will not be sufficient to do so in the not too distant future.

Government Oversight Play in Securing Patient Portals

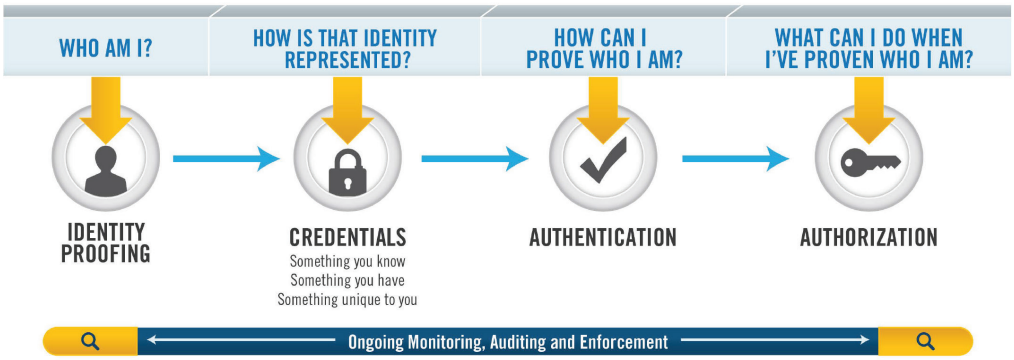
The Office of the National Coordinator for Health Information Technology (ONC), HIMSS (Healthcare Information and Management Systems Society), the National Institute of Standards and Technology (NIST), and even The White House increasingly recommend all patients go through an identity proofing process and be issued a multi-factor authentication credential before they access any of their medical records through a patient portal.

ONC

In its 2015 document entitled "A Shared Nationwide Interoperability Roadmap", ONC[4] states nationwide interoperability requires that all participants, regardless of role (e.g., individual, provider, researcher), be identified and authenticated to access a system so there is a high level of trust that participants cannot fraudulently pose as someone else. Identity proofing is the process of verifying that a user is who they say they are and binding a technical credential to that identity. (See figure below)



Authentication occurs when an individual or system uses a credential, such as a username and password, to access a system (See figure below)



In the opinion of ONC, appropriate identity proofing and authentication policies, processes and technologies can help individuals trust that their electronic health information and other data are secure and private. The HIPAA Security Rule includes an authentication standard that requires CEs to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. The National Institute of Standards and Technology (NIST) Special Publication 800-63-2 defines several levels of assurance (LoA), ranging from one to four, that outline requirements for establishing trustworthy identity proofing and authentication. Higher risk functions and services, such as access to electronic health information, require a higher LoA.

The Office of Civil Rights (OCR) — HIPAA Enforcement[5]

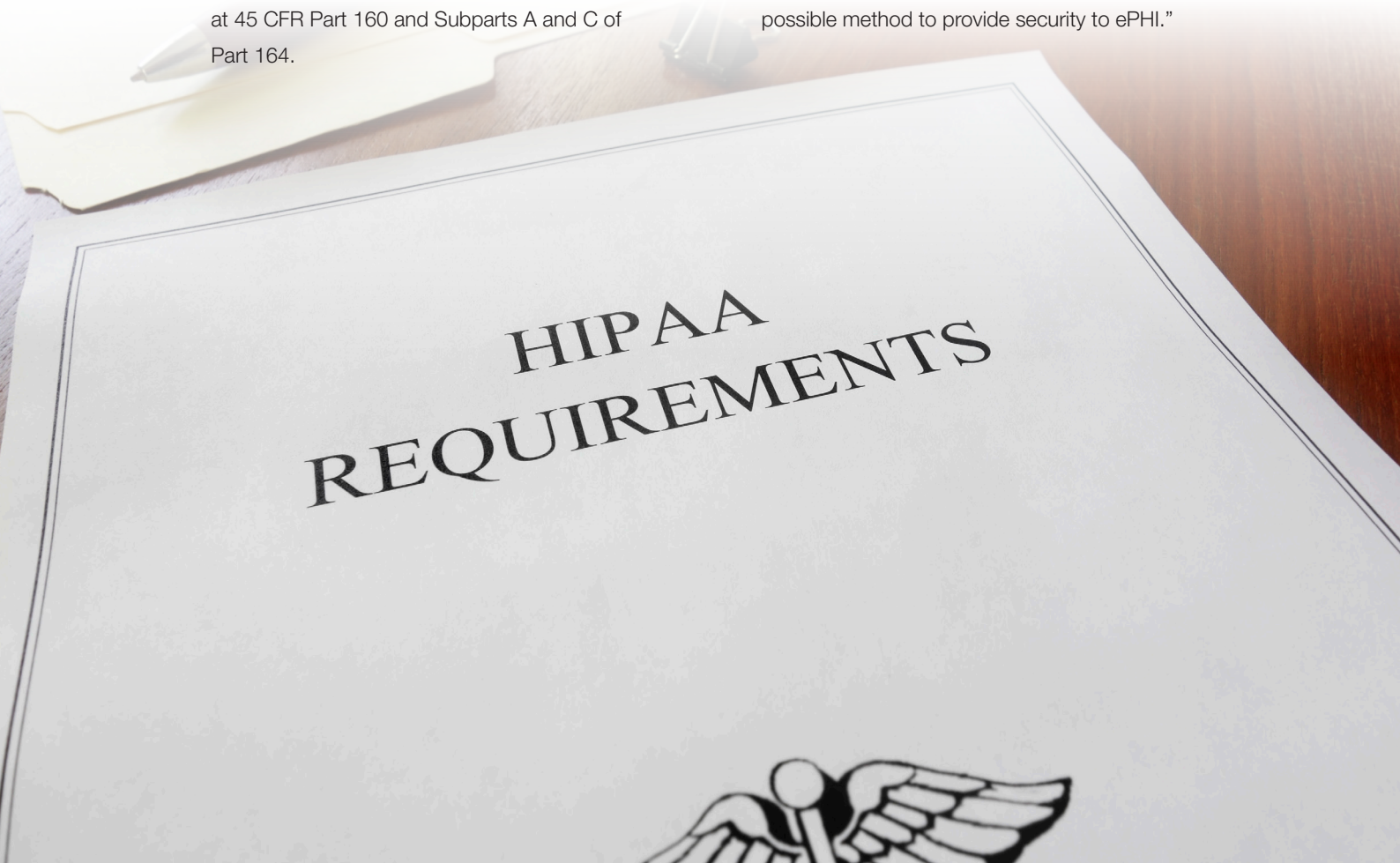
a. A set of federal standards to protect the privacy of patients' medical records and other health information maintained by covered entities and their business associates. Compliance with Privacy Rule required as of April 14, 2003 for most entities covered by HIPAA and by September 23, 2013 for their business associates.

b. The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

Note: while multi-factor authentication is not currently required, Covered Entities (CE) or Business Associate (BA) providing remote access for working with Protected Health Information (PHI), using multi-factor authentication should at least be considered. Having only a password, can be considered deficient in terms of meeting compliance with many of the HIPAA Security Rule subparts contained within

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

Meanwhile, ONC offers the following guidance: "HIPAA offers two-factor authentication as a possible method to provide security to ePHI."



HITECH Act Enforcement Interim Final Rule

The Health Information Technology for Economic and Clinic Health (HITECH) Act[6], enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

HIMSS' Guidance for Securing Patient Portals

The Healthcare Information and Management Systems Society's (HIMSS)[7] Identity Management Task Force (IDM TF) represents HIMSS membership with regard to national and industry initiatives on identity management, such as the National Strategy for Trusted Identities in Cyberspace's Identity Ecosystem Steering Group (NSTIC IDESG) and other national policy and technical efforts. In addition, the IDM TF develops tools and resources that will assist HIMSS members on identity management issues

HIMSS' Identity Management Task Force (IDM TF) has published guidance to deploy secure patient portals accessed by trusted identities. Among its 2015 recommendations: all mechanisms or processes that provide electronic access by patients to their own Protected Health Information (PHI, as defined by HIPAA), must be capable of employing user identity proofing and authentication at a high level of confidence, greater than or equal to National Institute of Standards and Technology (NIST) Level of Assurance (LoA) 3 or equivalent (as determined by a documented HIPAA risk analysis).

White House's Precision Medicine Initiative

The mission of the President's Precision Medicine Initiative (PMI)[8] is to enable a new era of medicine through research, technology, and policies that empower patients, researchers, and providers to work together toward the development of individualized care.

The longitudinal research study will collect genomic information, electronic health records, as well as lifestyle and environmental exposure data from 1 million or more U.S. volunteers.

Securing numerous terabytes of protected health information is critical to the success of the PMI. Realizing this, the White House has leveraged the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Included in the Framework are specific access control provisions:

1. Identity Proofing. PMI organizations should develop a policy for verifying the identity of users and contributors (e.g., participants and healthcare provider organizations), prior to granting credentials for access to or contribution of PMI data.

2. Credentials. PMI organizations should use innovative approaches for authentication so that over time they do not rely on username and password alone, and should use strong multi-factor authentication for users of PMI data.

3. Authentication. Risk-based authentication controls should flow from the organization's security risk assessment, and should be commensurate with the type of data, level of sensitivity of the information, and user type.

4. Authorization. Authorization controls should be granular enough to support participant consent and should limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 placed a number of requirements on HIPAA-Covered Entities (CEs) to safeguard the Protected Health Information (PHI) of patients, and to strictly control when PHI can be divulged, and to whom[9].

What are the Penalties for Violating HIPAA?

Since the Enforcement Final Rule[10] of 2006, the Department of Health and Human Services' Office for Civil Rights (OCR) has had the power to issue financial penalties (and/or action plans) to CEs that fail to comply with HIPAA Rules.

The penalty structure is tiered, based on the knowledge a covered entity had of the violation. The OCR will set the penalty based on a number of "general factors" and the seriousness of the HIPAA violation.

The four categories used for the penalty structure are as follows:

- **Category 1:** A violation that the CE was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
- **Category 2:** A violation that the CE should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
- **Category 3:** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation
- **Category 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

Each category of violation carries a separate HIPAA penalty. It is up to the discretion of the OCR to determine a financial penalty within the appropriate range. The OCR considers a number of factors when determining penalties, such as the length of time a violation was allowed to persist, the number of people affected and the nature of the data exposed. An organization´s willingness to assist with an OCR investigation is also taken into account.

The general factors that can affect the level of financial penalty also include prior history, the organization's financial condition and the level of harm caused by the violation. These factors could decrease or increase the financial penalty issued.

- **Category 1:** Minimum fine of $100 per violation up to $50,000
- **Category 2:** Minimum fine of $1,000 per violation up to $50,000
- **Category 3:** Minimum fine of $10,000 per violation up to $50,000
- **Category 4:** Minimum fine of $50,000 per violation

The fines are issued per violation category, per year that the violation was allowed to persist. The maximum fine per violation category, per year, is $1,500,000.

HIPAA Enforcement Highlights, 2016

In July 2016 the Department of Health and Human Services' Office for Civil Rights levied its largest fine ever against a provider organization, Advocate Health Care, for violations of the Health Insurance Portability and Accountability Act, or HIPAA. The OCR's enforcement also includes penalties against four other organizations, similarly reflecting the largest fines in its history[11]. Among those fined:

- **Advocate Health Care.** Fine: $5.5 million. Individuals affected: 4 million. OCR found substantial deficiencies in how Advocate conducted risk assessments of electronic protected health information; how it implemented policies, procedures and facility access controls to limit access to electronic health records; how it oversaw the safeguarding of ePHI by business associates; and how it safeguarded an unencrypted laptop left in an unlocked vehicle overnight.

- **Feinstein Institute for Medical Research.** Fine: $3.9 million. Feinstein, a wholly controlled subsidiary of Northwell Health that comprises 21 hospitals and more than 450 patient facilities and physician practices, agreed to pay the fine to settle potential HIPAA Privacy and Security Rule violations and undertake a substantial corrective action plan to bring its operations into compliance.

- **University of Mississippi Medical Center.** Fine: $2.75 million. UMMC agreed to settle multiple alleged HIPAA violations, specifically a breach of unsecured electronic protected health information affecting approximately 10,000 individuals. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach. UMMC also adopted a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

- **Oregon Health & Science University.** Fine: $2.7 million. The University signed a HIPAA resolution agreement and corrective action plan following two earlier breaches. The incidents involved a stolen laptop and use of cloud storage services without having a business associate agreement in place.

- **New York Presbyterian Hospital.** Fine: $2.2 million. In addition to the fine the hospital entered into a corrective action plan for unauthorized filming of two patients while participating in the "NY Med" television series. OCR said the violation was a result of flaws in NYP's judgment in allowing filming of the TV series. OCR found that NYP gave the network "virtually unfettered access to its healthcare facility," which created an environment where PHI could not be protected.

Healthcare: The Most "At Risk" Industry

When it comes to healthcare, PHI theft is on the rise. While HIPAA violations are, in many instances, "self-inflicted" due to lack of due diligence by the provider, covered entity or business associate, data breaches are mostly externally originated and directed.

According to the Ponemon Institute and its Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data[12], it's not without precedent that healthcare organizations and business associates believe they are more vulnerable than other industries to a data breach.

In this case perception is reality. A majority of healthcare organizations (69 percent) and business associates (63 percent) believe they are at greater risk than other industries for a data breach. According to the 2016 Cost of Data Breach Study released by IBM and the Ponemon Institute, the monetary losses that the healthcare field faces in the wake of a data breach are indeed more than double the average of all other industries.

The overall industry impact? Based on its own research Ponemon estimates that data breaches could be costing the healthcare industry $6.2 billion.

Ironically, those same numbers mirror a more troubling piece of news.

According to the Identity Theft Resource Center[13] so far in 2016, nearly 6.2 million records have been compromised — adding to the more than 851 million records exposed over the last decade. In addition:

- Of the more than 176.5 million medical and healthcare records exposed since 2005, slightly more than 1.5 million have been physically stolen since 2014. More than 131 million records have been exposed due to hacking since 2007 and 17.2 million have been exposed by Data on the Move.

- Employee error/negligence and inside theft resulted in a total of 371 healthcare-related breaches. The PHI of nearly 120 million Americans has been compromised since the 2009 Breach Notification Rule took effect as part of the HITECH Act. [14]

- According to the aforementioned 2016 Cost of Data Breach Study it costs the healthcare industry about $355 per record lost or stolen, compared to the average of $158 for all sectors. [15]

- Significantly, the cumulative effect is that security (or the lack of it) is the number one reason why participants said they would not use a patient portal.

Mobile Health Apps May Be Subject to HIPAA and Warrant Bank-level Security

If you are a covered entity or business associate and offer a mHealth (or mobile health) app that creates, receives, maintains and transmits PHI it is in your best interest to lock down the security of your app or risk a serious HIPAA violation.

If your mHealth app is developed, owned and managed by a covered entity, and the app involves the use or disclosure of protected health information, the covered entity must protect that information in compliance with the HIPAA Rules.

The Office of Civil Rights has recently begun to include business associates to the list of auditable organizations for HIPAA Audits. App developers may be subject to HIPAA compliance as a business associate if they are creating or offering the app on behalf of a covered entity (or to a contractor of a covered entity).

mHealth applications will change the way we manage our health and mobile apps in general are already changing the way business is done. Consumers / patients demand instant access to your services. Unfortunately, attackers are taking advantage of the many complexities created by the mobile ecosystem to exploit vulnerabilities, resulting in sophisticated fraud schemes and theft of sensitive data. Health data is especially attractive.

Security Intelligence reports common security flaws include:[16]

- Login-related weaknesses, such as being able to bypass the login prompt to perform functions like interacting with external Web applications and services;
- Allowing users to create weak passwords — or use no passwords at all.
- Mishandling of sensitive information, such as storing it locally and transmitting it over the network unencrypted;
- Malicious code injection, such as requests or queries that can trip up the app and cause it to divulge otherwise protected information;
- Cryptographic keys hard-coded into the app that can be accessed using mobile forensics tools.

For the app to be secure and useable, it is imperative to balance application security with user convenience. In addition, proper security controls must cover all core components of your mHealth app – communication, storage, platform, provisioning, interface and user.

Problems You Need to Solve

As electronic patient portals become commonplace, practitioners and providers require advanced solutions to reduce cybersecurity threats and to safeguard patient information[17]. These include implementing initial identity-proofing and strong, subsequent authentication; remote identity-proofing and mobile authentication; transitioning patients from username and static passwords to multi-factor authentication; and, of course, supporting the convergence of requirements around HITECH, HIPAA, Meaningful Use and Stage 2 audits.

VASCO's healthcare solutions allow organizations throughout the industry to overcome their most pressing challenges, including:

- Identity Proofing — on-site or remotely over any mobile device for users accessing EHR/EMR applications or patient portals
- Authentication — conferring credentials upon initial identity proofing and all subsequent logins.
- HIPAA and the HITECH Act compliance — protecting patient data to reduce risk and the imposition of penalties.
- Patient Identity Theft Risk Mitigation – responsibly shielding providers from fraud and preventing medical malpractice.
- Secure access to data — enabling usability without disrupting convenience for practitioners

How You Can Solve Them

VASCO offers a suite of identity and access management solutions for web-based and mobile healthcare applications (including EHRs, eRXs, HIEs, VPNs and patient portals) to help protect sensitive data and improve compliance posture. You can start your road to an interoperable healthcare system quickly, and with minimal resources thanks to the unique secure identity management platform provided by VASCO:

- Identity Protection and Validation
- Strong Authentication
- Secure Access
- Bank-level Mobile App Security and Frictionless Multi-Factor Authentication
- E-Signature

How VASCO Solutions Protect Patient Portals

Identity Protection and Validation
VASCO's Identity Proofing Service is offered as part of our holistic digital identity management solution for the healthcare community. We ensure the required technical, regulatory and logistical aspects of identity validation and credential issuing are in place before authorized parties begin using the multi-factor authentication protocols required by the DEA.

Our Identity Proofing and Validation solutions meet the NIST Special Publication 800-63 Assurance Level 3 requirements for multi-factor remote network authentication.

Strong Authentication
VASCO's MYDIGIPASS for Healthcare[18] is a comprehensive solution for healthcare organizations, EHR and patient portal access. From identity proofing and provisioning to secure login and fulfillment — all aspects of digital identity management are accounted for on a single, fully integrated platform.

Secure Access
Our broad range of DIGIPASS hardware and software authenticators[19], as well as our IDENTIKEY Authentication Server[20] and VACMAN Controller API[21], offer a turnkey solution for secure remote access to patient data, delivering unprecedented convenience for practitioners and hospital staff. We enable your staff to have one known identity, with one strong authentication method across all your applications.

Bank-level Mobile App Security and Frictionless Multi-Factor Authentication
VASCO's DIGIPASS for Apps[22] is a comprehensive software development kit (SDK) that natively integrates application security, frictionless multi-factor authentication and electronic signing into your mobile applications, enabling you to extend and strengthen application security, deliver unprecedented convenience to your users, and streamline application deployment and life cycle management processes.

Key Features include:
- Runtime Application Self Protection (RASP) — dynamically monitors application execution to detect and prevent attacks on mobile apps
- Geolocation — utilizes the location of a mobile device as a key risk analysis element
- Risk based authentication — real-time analysis that scores the risk profile of a transaction based on all of the available data points and can dynamically step-up security when necessary
- One-time Password (OTP) generation and validated by central server
- Biometric Authentication
  - Facial Recognition – utilizes face data points and liveliness detection to quickly & accurately authenticate users
  - Fingerprint- scan to quickly & accurately authenticate users

E-Signature
eSignLive is VASCO's e-signature solution for secure document signing processes that helps healthcare providers and partners to replace their outdated, paper-intensive processes for electronic records, while maintaining regulatory compliance. The Health Insurance Portability and Accountability Act (HIPAA) protects individually protected health information held by covered entities (CEs) and their business associates (BAs). eSignLive complies with all HIPAA requirements as they apply to business associates.

Why Choose VASCO?

VASCO is a global leader in trusted security with multi-factor authentication, transaction data signing, document e-signature and identity management solutions designed for all businesses and government agencies. More than 10,000 customers in 100 countries, including over half of the world's Top 100 banks, and over 350 healthcare organizations rely on VASCO to secure access, manage identities, verify transactions, simplify document signing and protect high value assets and systems.

VASCO also secures access to data and applications in the cloud and provides a robust toolset for application developers to easily integrate security functions into their web-based and mobile applications.

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.

When it comes to securing your electronic patient portal it's all about Trust. Do you trust your physicians, staff, even patients?

Trusted Digital Identities combined with Strong Authentication provide a meaningful foundation for all stakeholders:

Economic Benefits

- Enabling new types of transactions online
- Reduce costs for sensitive transactions

Improved Privacy Standards

- Offer citizens more control over when and how data is revealed
- Share minimal amount of information

Enhanced Security

- Fight cybercrime and identity theft
- Increased consumer confidence

As you weigh your options for solutions to secure your electronic patient portal consider the following select benchmarks in your decision making:

Complies with federal & state mandates

- FIPS 140-2, NIST, HIPAA, Meaningful Use, DEA / EPCS, ONC's Strategic Roadmap

Scalable and "future proof"

Balance between security and usability

- Protect your network, especially remote access
- Secure patient portals (web and mobile)

In sum, the continued, mandated enforcement of HIPAA regulations and the persistence of data breaches, especially in healthcare, enable Trusted Identities when coupled with Strong Authentication to provide a resilient and integrated defense strategy against short as well as long-term physician, patient and institutional risk.

Sources

1. https://www.healthit.gov/providers-professionals/faqs/what-patient-portal
2. Patient Portal Identity Proofing and Authentication, HIMSS Identity Management Task Force
3. ibid.
4. https://www.healthit.gov/newsroom/about-onc
5. http://www.hhs.gov/ocr/about-us/
6. http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule
7. http://www.himss.org/about-himss
8. https://www.whitehouse.gov/precision-medicine
9. http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096
10. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement
11. http://www.information-management.com/gallery/12-largest-fines-levied-for-hipaa-violations-10029563-1.html
12. http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1
13. http://www.idtheftcenter.org/breachestop6000.html
14. http://www.csoonline.com/article/2954917/cyber-attacks-espionage/personal-health-information-in-the-wrong-hands-can-be-painful.html
15. http://www.nuemd.com/news/2016/07/05/data-breaches-cost-medical-industry-millions-dollars
16. https://securityintelligence.com/common-mobile-app-vulnerabilities-you-may-be-overlooking
17. https://www.vasco.com/solutions/healthcare-information-security/securing-patient-portals.html
18. https://www.vasco.com/solutions/healthcare-information-security/mydigipass-for-healthcare.html
19. https://www.vasco.com/products/two-factor-authenticators/index.html
20. https://www.vasco.com/products/management-platforms/identikey-authentication-server.html
21. https://www.vasco.com/products/management-platforms/vacman-controller.html
22. https://www.vasco.com/products/application-security/digipass-for-apps.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

VASCO®
THE AUTHENTICATION COMPANY