PortalGuard®

Solution Brief

Managing Identity for HIPAA Compliance

Table of Contents

Facing the Authentication Challenges in Healthcare Applications

What Practitioners Expect

When it comes to managing electronic protected health information (ePHI), authentication is the key to security. Like unlocking the doors to their offices, doctors, nurses, and support staff must have the keys to verify their identities before gaining access to particular healthcare applications. HIPAA does not specify the technical requirements for how to unlock these digital doors.[1] Rather it focuses on mitigating the risks by considering end-to-end information security and requiring that practitioners be trained on how to secure their personal identities.[2]

Of course, both the medical and support staff value easy-to-use, HIPAA compliant, authentication solutions – the least restrictive ones for their particular tasks at hand. Herein lies the engineering challenge for delivering well-designed solutions. In a contemporary healthcare setting, practitioners often need to access multiple applications while seeing patients and updating medical records during their workdays. Requiring separate logins to each application not only impedes usability. It also slows down the pace of work and reduces productivity.

Ideally, practitioners should only have to provide their authentication credentials when essential, and then seamlessly access all of the healthcare applications they need to do their jobs. As far as practitioners are concerned, HIPAA-compliant authentication should not disrupt how work gets done.

---

[1] The National Institute of Standards and Technology (NIST) sets computer security standards for Federal agencies and publishes reports related to IT security. According to NIST, HIPAA requires that healthcare applications must "Implement procedures to verify that a person or entity seeking access to electronic protected health information (ePHI) is the one claimed." See: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 4.17. Person or Entity Authentication (§ 164.312(d)) [http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ nist80066.pdf] From a technical perspective, this is a very general rule where implementers have many options for designing appropriate solutions.

[2] The US Department of Health and Human Services publishes extensive guidance and educational materials on health information privacy and the HIPAA Security Rule. See: http://www.hhs.gov/ocr/privacy/ hipaa/administrative/securityrule/securityruleguidance.html for links to official resources. For an ongoing assessment of current issues regarding HIPAA and healthcare IT, see David Harlow's Health Care Law Blog, http://www.healthblawg.com/

What the IT Group Needs

Certainly the IT group maintaining healthcare applications within a medical setting needs to deploy an authentication solution that meets or exceeds the HIPAA mandate. At the same time, the IT group needs to provide a solution that adapts to the organizational workflows.

Today, it is essential to authenticate healthcare practitioners to the multiple applications running on an intranet, as well as support them when connecting from various PCs and mobile devices. The IT group requires a solution that enhances usability for authorized users, while sufficiently strong to provide the defense in depth against unauthorized people and processes gaining access to the protected applications. In addition, the IT group needs an audit-ready solution (should management questions arise) by continuously logging all authentication-related events.

Unobtrusive Authentication and Identity Management

Needed are systematic capabilities for unobtrusive authentication and identity management. A HIPAA-compliant solution should be able to authenticate to multiple applications running within a healthcare setting and also secure access from remote users and mobile devices. It should have the flexibility to manage authentication based on operational policies that expedite workflows and enhance productivity.

An effective HIPAA-compliant solution must strike the right balance between practitioners' needs for seamless authentication across multiple applications on one hand, and for mitigating risks on the other. A well-engineered solution optimizes both usability and authentication.

PortalGuard Solutions for Networked Healthcare Applications

Seamless Authentication That Adapts to the Environment

This is where PortalGuard makes a difference. It provides seamless authentication to ensure HIPAA compliance for networked healthcare applications. It is a flexible solution that adapts to the flow of work activities within a doctor's office, clinic, or other healthcare setting.

PortalGuard supports HIPAA-compliant authentication and event logging across different network configurations, including a LAN-based intranet, wide area access over the Internet, and connections from mobile devices. It leverages the underlying platform and enterprise architecture of either a Web powered or a native Windows-based application environment. It can be deployed in two modes, by:

- Adding identity management services to a Web-based environment to support Web-powered applications, or
- Replacing the out-of-the-box Windows Workstation authentication services to support native Windows applications

PortalGuard is infrastructure agnostic. It ensures identity management for ePHI applications running either on premise or 'in the cloud.'

Significantly, PortalGuard balances usability with security by managing when and where identity credentials are required for accessing multiple applications. It adapts state-of-the-art authentication technologies, including Two-Factor Authentication, Single Sign-On (SSO), and Password Synchronization, to the security needs and operational policies of a healthcare organization.

Making Two-Factor Authentication Seamless Yet Effective

Beyond the familiar capabilities of username/password challenges, Two-Factor Authentication strengthens and verifies identity claims by combining "some thing you know" with "something you have."[3] This second factor is a One-Time Password (OTP) retrieved from a hardware key fob, smartcard, proximity badge, mobile device, or telephone voice message. PortalGuard can be configured to accommodate numerous hardware- or software-generated OTP.

For example, a nurse seeking access to a healthcare application can be required to enter his username and password (something he knows) and then a hardware token generated One-Time Password (something he has). But there's a usability problem with repeated access. Adding this second factor to each username/password challenge can make repeated (and frequent) logins to the protected application a time-consuming and difficult-to-use effort. The nurse needs a solution that affirms his identity and expedites authentication to the application.

PortalGuard makes Two-Factor Authentication seamless by optionally storing the second factor for a period of time defined by the organization's security policies. (Illustration 1 shows the management options.) This verifies that the practitioner requesting access to an application is in fact using a predefined desktop, laptop, or mobile device.

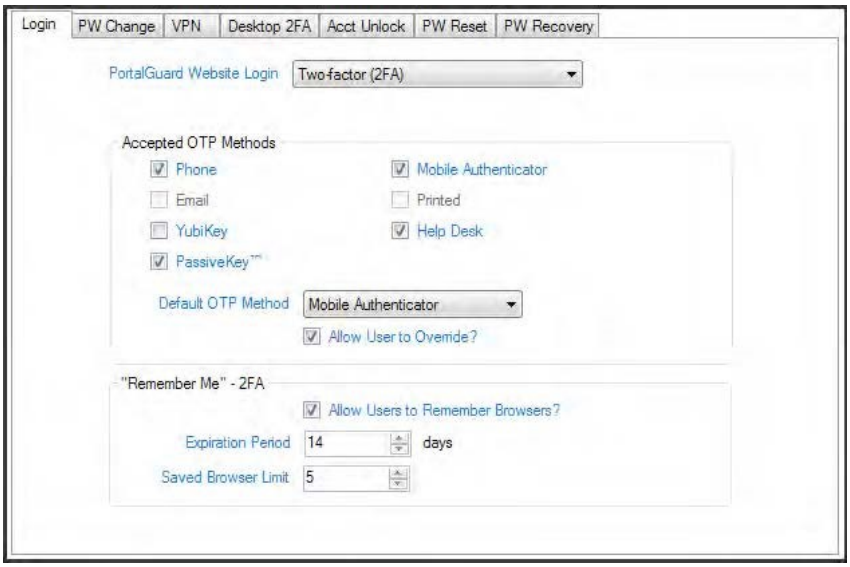

Illustration 1. Administrators can determine the expiration period for remembering the one time password for two factor authentication based on the security policy of their organization.

PortalGuard supports two separate methods for enhancing Two Factor Authentication: PassiveKey and PassiveKey Mobile. Systems integrators can implement the method that best suits the needs and policies of a particular healthcare setting.

[3] For an overall description of PortalGuard and Two-Factor Authentication, see http://www.portalguard.com/two-factor-authentication.html

PassiveKey

As a unique PortalGuard capability, PassiveKey is implemented as a web browser plug-in that is installed on workstations. It supports Internet Explorer, Firefox, and Chrome on Windows workstations. PassiveKey provides a transparent method for eliminating browser-based OTP prompts.

For example a doctor can use a smartcard as the second factor to login to her desktop machine. Once authenticated to Active Directory and Windows, PortalGuard with PassiveKey and SSO automatically authenticates the doctor to the various healthcare applications, even if they require Two-Factor Authentication.

PassiveKey Mobile

With PassiveKey Mobile, PortalGuard supports Two-Factor Authentication through any browser on any operating system. Once users authenticate manually with the second factor through a browser, PassiveKey Mobile remembers the second factor for a predefined period of time. This browser can be running on a tablet or smartphone, or accessed through desktop virtualization environment provided by Citrix or VMWare. To enforce policy-based authentication challenges, IT administrators can configure the expiration timeouts independently for different sets or types of users.

For example, after entering a second factor to authenticate at the beginning of her workday, a nurse simply needs to use her username/password credential to repeatedly access a web-based healthcare application from her tablet. The need to provide the second authentication factor is suppressed for as long as the time permitted by her organization's security policy.

Seamless Authentication To Linked Healthcare Applications

Practitioners often need to authenticate to multiple applications linked from a healthcare portal. Once authenticated to the portal, they expect direct access to these online resources. The portal needs to validate identities to ensure seamless access.

PortalGuard supports both Single Sign On (SSO) and Password Synchronization to ensure seamless authentication.[4]

- PortalGuard's SSO utilizes Security Assertion Mark-up Language (SAML), an open standard for web-based authentication where an authentication service (the "identity provider") runs within the network and authenticates access to multiple applications.
- Password Synchronization directly correlates external users' passwords for the portal with the passwords they need to access the linked applications. This is suitable for accessing legacy applications that do not support the standards-based approach for SSO.

[4] See additional resources on the PortalGuard web site for more technical information about Single Sign-On (http://www.portalguard.com/single-sign-on.html) and Password Synchronization (http://www.portalguard.com/passwordsynchronization.html)

In short, different applications have different authentication requirements and password challenges. PortalGuard has the flexibility to adapt to how applications need to work within a healthcare setting.

Logging Events for Audit Controls

PortalGuard maintains a continuous log of all authentication activities – both successful and unsuccessful events when logging into a protected healthcare application. The logging produces SQL-formatted data, which can then be easily exported and transferred to an auditing and reporting tool such a Crystal Reports.

Optimizing Identity Management for Business Value

Security and Usability

In short, a HIPAA-compliant authentication solution must be able to verify that the people and entities seeking access to a healthcare application are in fact who they say they are. This solution must be designed to mitigate the risks of unauthorized access.

At the same time, usability is an essential element of a well-engineered solution. Healthcare practitioners are accessing multiple networked applications during their workdays and need to authenticate seamlessly yet securely.

Striking the Right Balance

PortalGuard delivers HIPAA-compliant solutions for authentication that ensure security while enhancing usability. It provides a range of features that expedite access to networked healthcare applications while enforcing policy-driven security requirements. PortalGuard strikes the right balance between usability and strong authentication.

As a result, an IT group supporting doctors, nurses, and their staff can manage identities for accessing multiple applications within a networked environment. It can optimize authentication for usability. With this HIPAA-compliant solution in place, the IT group can refocus its attention on enhancing organizational work-flows, increasing productivity, and improving the overall quality of the healthcare applications available to practitioners on the network.