imprivata®

Nine Ways Imprivata Helps with HIPAA Compliance

Are You Ready for a HIPAA Audit?

HIPAA security and privacy requirements are nothing new to healthcare—they have been part of doing business for years now. But the HITECH act, introduced in 2009, significantly raised the stakes, and the Health and Human Services Office of Civil Rights is stepping up enforcement, contracting with KPMG to perform audits of 150 covered entities beginning in late 2011 and going into 2012 and beyond.

HIPAA compliance is more important than ever, but how can you be compliant with all the disparate systems you are managing? This whitepaper gives you nine ways Imprivata can prepare you before any HIPAA audit occurs—without impacting your end users.

OVERVIEW: NINE WAYS IMPRIVATA HELPS WITH HIPAA COMPLIANCE

	HIPAA Standard	How Imprivata Can Help
1.	Security Management Process Section Information System Activity Review; 164.308(a)(1)	✓ Streamline system activity reviews with centralized access/activity reporting and logs.
2.	Workforce Security 164.308(a)(3); Authorization and/or Supervision, Termination Procedures	✓ Centralize authorization—user and computer access controlled in one place. ✓ Single control to lock down network and application access upon employee departure.
3.	Information Access Management 164.308(a)(4); Access Authorization, Access Establishment and Modification	✓ Simplify setup and modification to user access with a single point of access control, authentication and authorization. ✓ Transaction-level strong authentication to support ePrescribing, chart signing or CPOE without disrupting the physicians workflow.
4.	Security Awareness and Training 164.308(a)(5)(ii)(C); Login Monitoring, 164.308(a)(5)(ii)(D); Password Management	✓ Centralize login monitoring and auditing of successful and failed login attempts. ✓ Simplify password management for care providers—no more multiple complex password rules.
5.	Security Incident Procedures 164.308(a)(6); Response and Reporting	✓ Proactively report and alert on suspicious login events for failed attempts.
6.	Workstation Security 164.310(c)	✓ Lock workstation when care provider walks away preventing unauthorized access to PHI from unattended workstations.
7.	Access Controls Unique user identification; 164.312(a)(2)(i), Automatic Logoff; 164.312(a)(2)(iii)	✓ Prevent credential sharing and users writing down passwords. ✓ Lock workstations when authorized user leaves.
8.	Audit Controls 164.312 (b)	✓ Centralize audits of all workstation and application access by users.
9.	Person or Entity Authentication 164.312(d)	✓ Implement strong authentication choosing from a broad range of technologies (badges, biometric, etc...).

IMPRIVATA IN HEALTHCARE

Meeting HIPAA compliance when managing multiple disparate systems can be complex. Each system audits and sets up credentials differently, creating overhead and complexity for IT. Imprivata OneSign® combines strong authentication, and single sign-on to create a single point of access management, password policy, and compliance reporting for all desktops and applications. OneSign is widely deployed in hospitals and healthcare organizations, where the need for streamlined access to electronic health records is balanced by the need for stringent security and privacy.

Imprivata has helped over 1,000 healthcare organizations around the globe successfully address the challenges of protecting, controlling, and auditing access to patient information in applications without impacting the end user experience.

Addressing Specific Challenges of Healthcare

While the specifics of how you address HIPAA will vary depending on your environment, applications, and employees, you must consider the overall environment in which compliance occurs. OneSign helps you address HIPAA compliance without putting an undue burden on IT or clinical providers by ensuring:

- ***Physician adoption:*** With the HITECH Act, physicians are making significant changes in how they do their jobs. Security measures like strong passwords often increase the burden on the physician, and can delay EMR adoption. OneSign improves physician workflow, lowering potential barriers to EMR adoption.
- ***Simplified, centralized authentication management:*** Many healthcare organizations use a mix of applications, including legacy systems that cannot easily be modified to support strong authentication or other security measures. OneSign works with virtually any application and is easy to deploy and maintain while delivering the fastest authentication, and SSO user experience.

NINE WAYS IMPRIVATA CAN HELP WITH HIPAA COMPLIANCE

1. Security Management Process: Streamline system activity reviews

The Security Management standard requires covered entities to implement policies to prevent, detect, contain, and correct security violations. Implementation specifications for this standard include Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review.

Clearly this standard involves policies and procedures that are much broader than an underlying technology, such as performing a broad risk analysis.

How Imprivata can help:

- **Centralize and streamline audit reporting:** Aggregating and reviewing audit logs, access reports, and security incident reports across multiple systems can be tedious and time-consuming, OneSign keeps all system access logs and activity records in one place, simplifying your information system activity review.

2. Workforce Security: Centralize Authorization

The Workforce Security standard dictates that, for each workforce member or job function, the covered entity must identify the EPHI that is needed, when it is needed, and make reasonable efforts to control access to EPHI. The three implementation specifications include Authorization and/or Supervision, Workforce Clearance Procedures, Termination Procedures.

How Imprivata can help:

- **Centralize authentication:** OneSign® Authentication Management offers an appliance-based identity management with built-in support for enforcing strong authentication policies. Imprivata OneSign strengthens user authentication at the desktop, network, application, and transaction level by replacing weak Windows desktop and remote VPN passwords with a broad range of strong authentication options, including finger biometrics authentication, proximity cards, and smart cards.
- **Single control to lock down upon employee departure:** Administrators can easily monitor and control employee access to EPHI, and automatically lock down all user network and application access upon employee departure or termination by controlling their single sign-on access.

3. Information Access Management: Simplify setup and modification to user access

A basic rule of security is enforcing 'least privilege' access – or ensuring that only individuals with a need for access to EPHI can access it. The three implementation specifications for this standard include Isolating Healthcare Clearinghouse Functions, Access Authorization, Access Establishment and Modification.

How Imprivata can help:

- **Single point of control for access, authorization, and authentication:** Aside from helping you with the access authorization and access establishment/modification implementation Imprivata makes it easy to assign access privileges based on groups and needs, and to track exactly who has been authorized for which application. Access rights can be easily modified to a specific application or all applications from a single centralized interface.
- **Transaction level strong authentication:** Using the OneSign ProveID web services API, developers can integrate transaction-level strong authentication and verification into the ordering process and/or utilize OneSign for authentication from proprietary endpoints and devices.

4. Security Awareness and Training: Centralize monitoring and auditing; Simplify passwords

Implementing the best security policies is useless if employees/contractors do not follow them. The Security Awareness and Training standard is meant to address this issue, requiring covered entities to provide training for all members of the workforce. Implementation specifications include Security Reminders, Protection from Malicious Software, Log-in Monitoring, Password Management.

How Imprivata can help:

- **Log-in monitoring:** OneSign monitors both successful and failed attempts at user, desktop, and application login. It has the ability to generate notifications and reports for successive failed login attempts.
- **Password management:** Using OneSign® Single Sign-On, you can manage and enforce password policies uniformly across all applications, including applications that do not directly enforce your policies for password change or complexity. OneSign takes care of all passwords, and even lets you obscure passwords to sensitive applications from users, so they can only access the application using their OneSign credentials. With the single sign-on capabilities of OneSign, users have no need to write down or otherwise compromise passwords, as they only need to enter a password once to access all of their authorized applications. Obscured passwords restrict the users access when they are remote.

5. Security Incident Procedures: Proactively report and alert on suspicious events

The Security Incident Procedure standard requires that covered entities implement policies and procedures for security incidents. The required implementation specification involves response and reporting, meaning you must be able to identify and respond to security incidents as they occur.

How Imprivata can help:

- **Track suspicious events:** OneSign reports and alerts on suspicious events, such as multiple failed login attempts from a single account or an attempted login from a remote account when the user is already logged in on premise and detecting account sharing or password sharing.
- **Automatic lock down of accounts:** In the case of an intrusion, OneSign has the capability of locking down access for all users.
- **Report on user login credentials:** In one place see workstation and application credentials.

6. Workstation Security: Automate workstation locking

The Workstation Security standard requires that you have policies and procedures in place to protect workstations and restrict unauthorized access to EPHI.

How Imprivata can help:

- **Automate workstation locking:** OneSign Secure Walk-Away® helps demonstrate adherence to this standard by locking down access to EPHI on the network when the authorized user walks away. OneSign also supports inactivity timers and random challenges. It uses active presence detection and facial recognition technology to automatically lock the session when the authorized user walks away. OneSign also supports inactivity timers and random challenges. Since EPHI resides within the application (not the workstation itself), and access is not possible without authorization, this effectively prevents a vulnerable workstation from becoming a gateway to protected health information.

7. Access Control: Prevent credential sharing and automate workstation locking

The Access Control standard requires covered entities to create processes and policies to ensure that individuals only have access to the EPHI for which they have been granted access, based on roles or responsibilities.

How Imprivata can help:

- **Unique user identification:** Using OneSign, you can prevent users from sharing credentials, particularly if you add a second authentication factor such as a badge or fingerprint biometric that is unique to each individual.
- **Automatic logoff:** It is critical to ensure that EPHI on unattended workstations is not exposed to unauthorized personnel. OneSign supports time-outs and hotkeys, but these only go partway to addressing the problem leaving you at some risk to forgotten hotkeys or interrupted timeouts. With OneSign Secure Walk-Away, the session is locked as soon as the physician walks away – and unlocks automatically on the physicians return, bringing them back to where they were.

8. Audit Controls: Centralize audits of all workstation and application access

The Audit Control standard requires organizations to implement mechanisms for auditing the activity in information systems containing EPHI. In the healthcare environment, where many different applications may contain EPHI, managing and maintaining audit trails can be tedious.

How Imprivata can help:

- **Centralize audits:** Imprivata OneSign provides a complete record of all workstation and application access in one place, simplifying auditing and reporting by centrally auditing.

9. Person or Entity Authentication: Implement strong authentication

The Person or Entity Authentication standard requires covered entities to implement procedures to ensure that someone is who they claim to be, before granting access to EPHI. Using passwords alone to authenticate individuals is the most common approach, yet the least desirable in healthcare for many reasons.

- Passwords are notoriously insecure; users often use the same simple passwords across different applications, or when forced to use strong passwords, they often write them down.
- In the healthcare environment, the time spent typing passwords to authenticate with each application delays access to patient data, and causes physician frustration.

How Imprivata can help:

- **Multiple authentication technologies:** Imprivata OneSign combines multiple authentication technologies with single sign-on, enabling stronger authentication without getting in the way of how physicians deliver patient care.

- **Broad range of authentication options:** OneSign Authentication Management supports finger biometrics, active and passive proximity cards, smart cards, one-time passwords, USB tokens, and phone-based authentication. Combining multiple authentication factors makes theft or misuse very difficult, while single sign-on reduces the burden of authentication for each application.

LEARN MORE ABOUT IMPRIVATA IN HEALTHCARE

For more information on OneSign customers and applications in healthcare, visit http://www.imprivata.com/healthcare

ADDITIONAL INFORMATION

HIPAA compliance is a broad subject involving people and processes as well as technologies. This paper is not meant to provide comprehensive guidelines to HIPAA compliance. For more information on the broader compliance effort see the following resources:

- NIST SP 800-66: Introductory Resource Guide for Implementing the HIPAA Security Rule
- PA Checklist for HIPAA & HITECH Compliance Mandates
- U.S. Department of Health & Human Services Health Information Privacy
- Department of Health and Human Services Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule
- Security 101 for Covered Entities
- HIMSS
- Center for Medicare & Medicaid Services

Worldwide Headquarters
10 Maguire Road, Building 4
Lexington, MA 02421-3120 USA
Phone: 781 674 2700
Toll-free: 1 877 ONESIGN
Fax: 781 674 2760

www.imprivata.com