



Achieving HIPAA Compliance with Enterprise Single Sign-On

TABLE OF CONTENTS

The Challenges of HIPAA Compliance	3
Costly and Complex	3
Increased User Frustration.....	3
More Guidance Needed.....	3
How the Right Enterprise Single Sign-On Solution Can Satisfy HIPAA	
Security Requirements	4
Technical Safeguard Standards	4
Administrative Safeguard Standards.....	5
Physical Safeguard Standards.....	6
Achieving HIPAA Compliance With Imprivata® OneSign™	6
How Imprivata OneSign Works.....	7
OneSign Enrollment and Deployment	7
The OneSign User Experience.....	7
Beyond HIPAA Compliance –	
Other Advantages ESSO Delivers to Healthcare Providers	8
Learn More	9

The Challenges of HIPAA Compliance

When the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996, among the law's many provisions was the establishment of formal regulations designed to protect the confidentiality and security of patient information. Congress set a series of deadlines for healthcare institutions to comply with the new regulations, including an April 2005 deadline for compliance with the security requirements.

In addition to mandating new policies and procedures, the HIPAA security regulations require mechanisms for controlling access to patient data on healthcare providers' information technology (IT) systems. Two and a half years after the April 2005 deadline for meeting these IT security and access management requirements, many providers and institutions are still struggling to achieve compliance.

Key challenges for healthcare organizations continue to include:

Costly and Complex

- Most hospital IT environments include a broad mix of legacy, PC and Web applications. Any access control methods they employ must address all applications and platforms in their environments — as well as connections from remote locations.
- Many legacy systems have been around for a long time. Hospital IT organizations lack the resources or lack access to the code required to modernize them or adapt them to new regulations.
- Many healthcare IT organizations lack the budget to undertake any HIPAA-related projects that would require large capital outlays. Even when money is available for these projects, development and deployment of enterprise-wide access control mechanisms often require months or years of effort.

Increased User Frustration

- As the number of applications grows, the number of passwords that each employee must remember also grows. Whenever an employee forgets a password, help desk teams - already strained from budget cuts and reduced staffing – need to devote time and resources to resolving the problem. User frustration intensifies while productivity drops. Neither is acceptable in dynamic healthcare environments where timely and convenient access to information are critical to patient care.
- Many access control methods, such as strong password policies, put the burden of compliance on the users by requiring them to memorize multiple complex passwords or change them frequently. This leads to more forgotten passwords and more help desk calls. Physicians and hospital staff are pushing back and resisting HIPAA requirements they perceive to be “too onerous.”

More Guidance Needed

- The Office of Civil Rights in the U.S. Department of Health and Human Services, the government body responsible for enforcing the HIPAA regulations, has published the requirements for HIPAA compliance. Healthcare providers need to figure out for

themselves “how” best to meet those requirements. Many IT professionals are left wondering how much is enough or too little.

- Vendors who make false or exaggerated claims that their software solutions are “HIPAA-compliant” or “government-certified” further confuse IT organizations. In fact, no government certification program for HIPAA compliance exists. Each healthcare organization needs to establish its own certification process.

In response to these challenges, a growing number of healthcare institutions are turning to Enterprise Single Sign-On (ESSO) solutions to help them comply with HIPAA’s security requirements. ESSO solutions require a user to remember and provide just one set of credentials—username and password or a fingerprint—to access the full portfolio of applications, data, and services for which that user is authorized.

How the Right Enterprise Single Sign-On Solution Can Satisfy HIPAA Security Requirements

To achieve HIPAA compliance, organizations need to adopt and enforce a range of policies, processes and procedures. ESSO solutions can help ensure the success of these initiatives. However, the technologies, capabilities, costs and requirements of ESSO solutions vary greatly. In order to select the right ESSO solution, healthcare providers should look for products that address key aspects of HIPAA security requirements.

HIPAA SECURITY STANDARDS

The following tables detail the HIPAA requirements that a proper ESSO solution must address:

Technical Safeguard Standards

Access Control	Section 164.312	ESSO should support:
Unique User Identification	Section 164.312 (a)(1)	Multiple users signing on to a shared workstation without logging out of the desktop. Identify which users are sharing credentials.
Automatic Logoff	Section 164.312 (a)(1)	Providing uniform automatic logoff across applications.
Audit Controls	Section 164.312 (b)	Centralized auditing of all application access events down to the screen level.
Person or Entity Authentication	Section 164.312 (d)	Enabling a broad selection of strong authentication options such as biometrics and security tokens for positive verification of identity prior to system access.

Administrative Safeguard Standards

Security Management Process	Section 164.308 (a) (1)	ESSO should support:
Information System Activity Review		Enabling the review of system activity via logs that show user time in and time out. Works in conjunction with application logs to doubly-verify user activity. These audit logs are essential for any Access Control Risk Analysis or Risk Management effort.
Workforce Security	Section 164.308 (a) (3)	ESSO should support:
Authorization and/or Supervision		Enforcing network-level authorization.
Termination Procedures		Providing a mechanism for enforcing network-level authorization.
Information Access Management	Section 164.308 (a) (4)	ESSO should support:
Access Authorization		Enabling a single point of control for access, authorization and authentication.
Access Establishment and Modification		Comprehensive access audit logs and the ability to modify access rights. Establishing a single point of control for denying network systems and application access.
Security Awareness and Training	Section 164.308 (a) (5)	ESSO should support:
Login Monitoring		Centralized monitoring of login attempts (success and failure) at a user, desktop, and application level.
Password Management		Assisting the management of password policies via implementation of strong passwords at one central point. Allowing uniform password standard across organization, even if the application doesn't support it. Obscuring passwords from end users.
Security Incident Procedures	Section 164.308 (a) (6)	ESSO should support:
Response and Reporting		Locking out or suspending user access if suspected security events occur. Logging and notifying the entity of such events.

Physical Safeguard Standards

Device Standards	Section 164.310 (c)	ESSO should support:
Workstation Security		Ensuring unoccupied workstations are automatically secured to prevent unauthorized access.

Achieving HIPAA Compliance With Imprivata® OneSign™

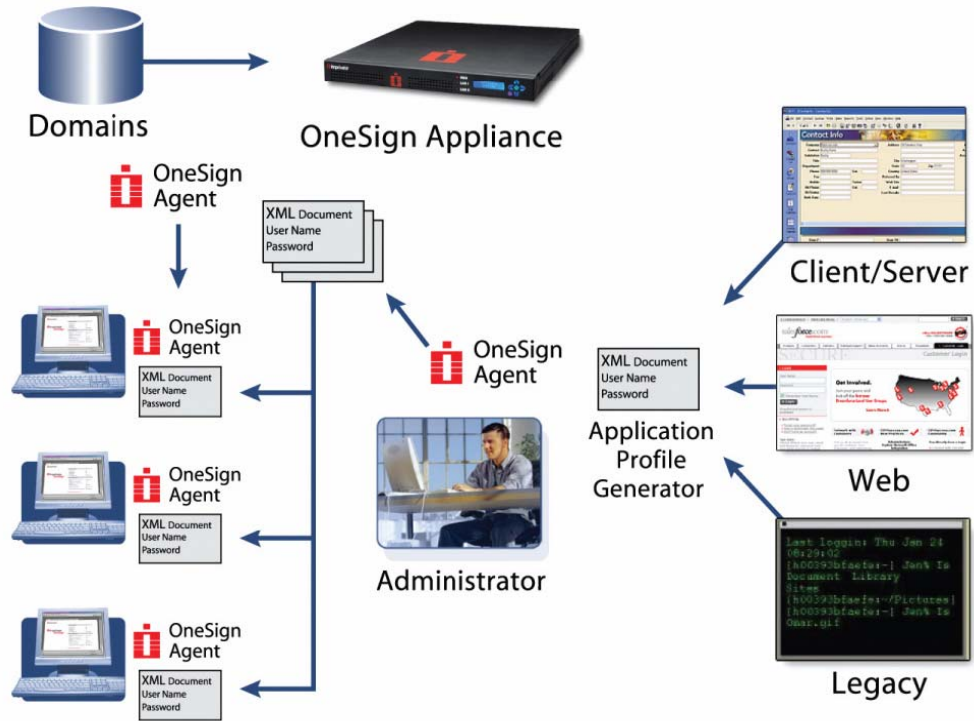
Healthcare providers can support HIPAA privacy and security requirements by strengthening application password security and establishing a log of user application access data. Imprivata® has helped hundreds of healthcare organizations around the globe successfully address these needs with an award winning solution recognized by KLAS® as “Best Single Sign-On Solution for 2006.”

Imprivata OneSign™ is an affordable, appliance-based approach that enables healthcare providers to implement ESSO for healthcare applications from Cerner, Epic, Meditech, McKesson, Siemens, and many more– including single sign-on to all Web-based, client/server and legacy applications. Through a centralized approach to password management, OneSign makes secure single sign-on services quick to deploy, and easy to administer. OneSign makes it simple and practical for healthcare institutions of all sizes to adopt and enforce password and strong authentication policies that support HIPAA compliance–not to mention significantly improve the clinician’s user experience and convenience.

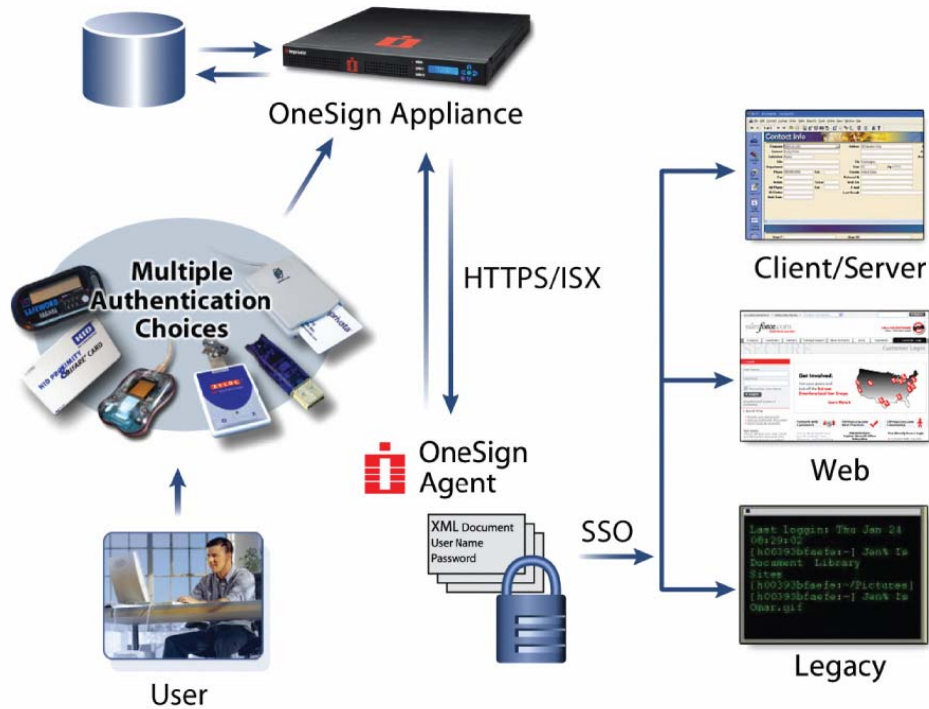
According to OneSign design partner, Christopher Paidhrin, IT Security Officer for Southwest Washington Medical Center, “To be HIPAA compliant when you have back-end legacy systems is very difficult, because application vendors must be forced into authentication and authorization compliance. Healthcare organizations need a password authentication scheme that proxies, that is, comes between, all the legacy systems and the user interface. OneSign provides exactly that service, allowing organizations to jumpstart HIPAA compliance. With OneSign, the IT department can bring everyone to a common organizational and healthcare industry standard of strong passwords, and eventually move to biometrics and/or two token authentication.”

How Imprivata OneSign Works

OneSign Enrollment and Deployment



The OneSign User Experience



Beyond HIPAA Compliance – Other Advantages ESSO Delivers to Healthcare Providers

A well-designed ESSO solution needs to support the unique requirements of healthcare environments:

- Shared workstation support: Additional users should be able to sign on to a shared workstation without logging out the first user. One button lock/unlock and single sign-on/off should also be supported.
- User accountability: The ESSO solution needs to record user access events and log files providing detailed reports on application access by user and by application.
- Support for authentication modalities: The ESSO solution should provide built-in support for major forms of strong authentication, including strong passwords, ID tokens and finger biometric technology.
- Universal application support: The ESSO solution must enable healthcare institutions to support single sign-on to any application, including popular healthcare solutions, such as Meditech, Cerner, McKesson and Med2020, Epic, Siemens, and others

Once organizations have evaluated potential ESSO solutions against HIPAA requirements– as well as other essential factors, such as cost and deployment requirements– they are likely to be looking at a much shorter and more manageable list of potential ESSO solutions.

Imprivata OneSign provides distinct and practical support for helping organizations demonstrate compliance with key sections of HIPAA, but the advantages of OneSign extend far beyond compliance.

With OneSign, organizations benefit from increased user productivity, convenience, and speed of access to information– critical in dynamic clinical environments where user workflows often require accessing multiple sets of data on a shared workstation and/or roaming from workstation to workstation.

With OneSign’s built-in support for a broad range of strong authentication devices, healthcare organizations can opt to replace passwords altogether with finger biometrics, or make use of proximity badges popular in many clinical settings. In addition, OneSign integrates with Fusion from Carefx™ to create a user driven, patient-centered workspace that synchronizes record context across multiple applications, increasing user productivity and patient safety. Lastly, third party provisioning systems can provision and de-provision application accounts within OneSign automatically, increasing “day-one” user productivity and ensuring that application credentials in OneSign are always up-to-date.

Imprivata OneSign provides an easy, simply smart, and uniquely affordable enterprise single sign-on solution that delivers rapid ROI, increased user productivity and convenience, and regulatory compliance. It’s the solution that is changing single sign-on in healthcare.

Learn More

To learn more about HIPAA compliance, visit:

<http://www.cms.hhs.gov/HIPAAGenInfo/>

<http://www.hhs.gov/ocr/hipaa/>

<http://www.hipaadvisory.com/>

To learn more about Imprivata OneSign, please visit

Our website at <http://www.imprivata.com>

Send an email to our sales team at sales@imprivata.com

Call us at 877ONESIGN.



10 Maguire Road
Building 4
Lexington, MA 02421
v 781 674 2700
f 781 674 2760

Imprivata EMEA
Forsyth House
77 Clarendon Road
Watford
Herts, WD17 1LE
United Kingdom
v +44 (0)1923 813 511
f +44 (0)1923 813 501

Imprivata APAC
#01-03 60 Cambridge Road
Singapore 219757
v +65 82 004 840

1.877.ONESIGN
www.imprivata.com
sales@imprivata.com