



The Value of Enterprise SSO to HIPAA Compliance

By
David Ting
Founder and Chief Technical Officer
Imprivata, Inc.

TABLE OF CONTENTS

Executive Summary.....	
.....	2

Ways in Which the Right ESSO Solutions Satisfies HIPAA Security Requirements.....	3
--	----------

HIPAA Security Standards.....	3
.....	

Other Advantages ESSO Should Deliver to Healthcare Providers.....	5
.	

Imprivata OneSign's Advantages for HIPAA

Compliance.....	5
------------------------	----------

How OneSign Works.....	
-------------------------------	--

.....	6
-------	----------

The Advantages of OneSign Over Other ESSO Solutions.....	
---	--

.....	7
-------	----------

Beyond HIPPA Compliance.....	
-------------------------------------	--

.....	8
-------	----------

The Value of Enterprise SSO to HIPAA Compliance

Executive Summary

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 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. As the April 2005 deadline draws closer, meeting these IT security and access management requirements is proving to be a challenge for many institutions, for a number of reasons, including:

- Complex IT environments:

Most hospitals' IT environments include a diverse assortment of legacy, PC and Web applications, both internal and external. Any access control methods they employ must address all applications and platforms in their environments.

- Complex legacy applications:

Many healthcare institutions still rely heavily on legacy systems for which the software code has grown increasingly complex over time. In many cases, institutions lack the resources to modify application code written years or decades earlier.

- Unchartered Territory:

While the government body responsible for enforcing the HIPAA regulations, the Office of Civil Rights in the U.S. Department of Health and Human Services, has published the requirements for HIPAA compliance, it has left it to the discretion of healthcare providers to determine how best to meet those requirements.

- Overburdened IT departments and help desks:

As the number of internal and external applications grows, so does the number of passwords that employees must remember. Every time an employee forgets a password, IT departments and help desks, already strained from budget cuts and reduced staffing, must devote time and resources to resolving the problem. At the same time, user frustration intensifies, and productivity drops.

- Cost: Many healthcare IT organizations lack the funding to undertake any HIPAA-related projects that would require large capital outlays.

- Time: Development and deployment of enterprise-wide access control mechanisms can often require months or years of effort, thus precluding the possibility of organizations meeting the April 2005 compliance deadline.

- User cooperation:

Many access control methods, such as strong password policies, can put much of the burden of compliance on application users by requiring them to memorize multiple complex passwords and change them frequently. Institutions are likely to encounter increased help desk calls regarding forgotten passwords, as well as resistance from physicians and hospital staff if the user requirements of HIPAA compliance are perceived as too onerous.

Copyright © 2005 Imprivata, Inc.

The Value of Enterprise SSO to HIPAA Compliance

To compound these challenges, a number of vendors have made false or exaggerated claims that their software solutions are "HIPAA compliant" or "government-certified." In fact, there is no government certification program for HIPAA compliance and each healthcare organization must 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—user name and password—to access the full portfolio of applications, data, and services for which that user is authorized.

Ways in Which the Right ESSO Solution Satisfies 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.

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

HIPAA Security Standards

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.
Workforce Security	Section 164.308 (a) (3)	ESSO should support:
Authorization and/or Supervision		Enforcing network level authorization.
Workforce Clearance Procedures		Providing a mechanism for enforcing network level authorization.
Termination Procedures		Simplifying the Authorization, Authentication, and Accountability aspects of network security policies and procedures.
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		Providing a gateway to role or policy based systems. Establishing a single point of control for denying network systems and applications.

Copyright © 2005 Imprivata, Inc.
The Value of Enterprise SSO to HIPAA Compliance

Security Awareness and Training	Section 164.308 (a) (5)	ESSO should support:
Login Monitoring		Monitoring of login attempts (success and failure) for training assessment. Demonstrating of trends for awareness assessment, e.g., is a user or department more likely to have failed login attempts? Are accounts being used?
Password Management		Assisting the management of password policies via

		implementation of strong passwords at one central point. Allowing uniform passwords it. Results in better management and greater security.
--	--	---

PHYSICAL SAFEGUARDS STANDARDS

		ESSO should support:
Workstation Use	Section 164.310 (b)	Providing a single point of control for access, authorization and authentication.
Workstation Security	164.310 (c)	Providing a mechanism for enforcing network-level authorization.

TECHNICAL SAFEGUARDS STANDARDS

Access Control	Section 164.312 (a) (1)	ESSO should support:
Unique User Identification		Assigning one set of unique user credentials for each individual that will allow access to Enables sharing of workstations without compromising security.
Automatic Logoff		Providing uniform automatic logoff across applications.
Person or Entity Authentication	Section 164.312 (d)	Enabling of positive verification of system use via biometric and token authentication. S
Transmission Security	Section 164.312 (e) (1)	Providing the security measures to guard against inappropriate access. No user can ac

To learn more about HIPAA compliance, visit:

<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>

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

<http://aspe.hhs.gov/admsimp/nprm/seclist.htm>

<http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>

Copyright © 2005 Imprivata, Inc.

The Value of Enterprise SSO to HIPAA Compliance

Other Advantages ESSO Should Deliver to Healthcare Providers

The proper ESSO solution should also support the unique requirements of healthcare environments

with the following capabilities:

- . • Shared workstation support:
Multiple users should be able to sign on to a shared workstation without logging out of the desktop. One button lock/unlock and Single signon/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 SSO on any application, including popular healthcare solutions, such as Meditech, Cerner, McKesson and Med2020.

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. One product on that list will be Imprivata OneSign.

Imprivata OneSign's Advantages for HIPAA Compliance

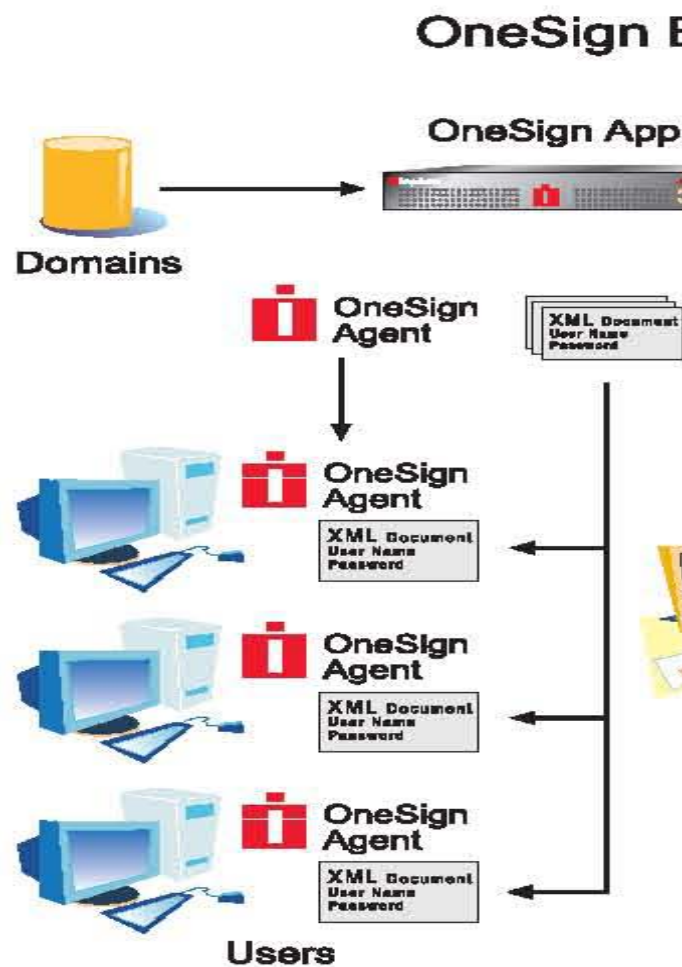
Two major ways in which healthcare providers can support HIPAA privacy and security requirements are by strengthening application password security and establishing a log of user application access data. An enterprise SSO solution can fulfill these needs, but some SSO solutions are costly, difficult and timeconsuming to deploy.

Imprivata OneSign is an affordable network appliance that enables healthcare providers to implement enterprise SSO for Web, client/server and legacy applications. Through a unique, centralized approach to password management, OneSign makes secure SSO services quick to deploy, convenient to use and easy to administer. OneSign makes it simple and practical for healthcare institutions of all sizes to adopt and enforce password policies that support HIPAA compliance.

According to OneSign design partner Christopher Paidhrin, Senior Systems Consultant at Superior Consultant Co. Inc., "To be HIPAAcompliant when you have backend 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 IS 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."

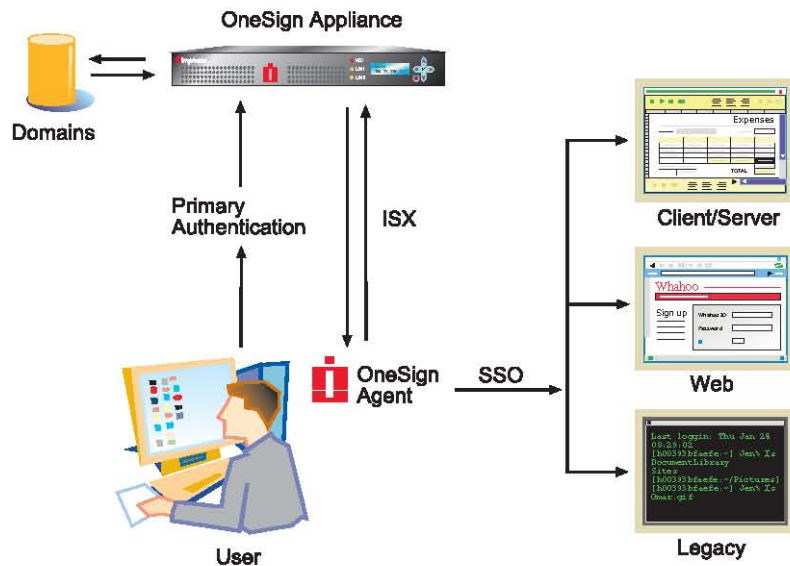
How OneSign Works

OneSign consists of three primary components: a central OneSign application server; a network of lightweight software agents; and the OneSign Agent Generator™ (APG) tool.



During deployment, the APG tool learns about the user's environment, including Web and legacy—and then uses that information to generate the XML documents. The XML files are then sent to the OneSign application server and stored centrally on the OneSign application server.

The OneSign User Experience



OneSign performs primary authentication using an extension of the Windows domain login. The OneSign agent then establishes an Imprivata Secure Exchange™ (ISX) session with the appliance using double-blind encryption and disposable session keys. ISX delivers the SSO data. The OneSign agent then observes the application screens as defined in XML, adopting the logon behavior necessary to enable SSO and password management according to the latest policy.

The Advantages of OneSign Over Other ESSO Solutions

- Easy to install, deploy, and maintain
- Non-disruptive to IT departments and users
- Works with legacy, client/server and Web applications without requiring code changes
- Lower cost and quick ROI

OneSign customer Burt Ridge, CIO at Laughlin Memorial Hospital puts it this way, "We looked at a dozen ESSO solutions. We found that many products were simply shifting the burden from the help desk back to IT, because they required an experienced, and therefore highly-paid, network or database expert for administration. And many of these solutions required extensive code changes to back-end applications. We also discovered that a large number of ESSO solutions were expensive to deploy and to maintain. We were very pleased when we found OneSign. It has made everyone more productive—IT staff, help desk personnel, physicians and hospital staff. This results in reduced costs and greater efficiency."

Mr. Paidhrin notes, "OneSign has advantages for both security and privacy. The return on investment is very quick, especially in the elimination of lost passwords, and the reduction of help desk calls. Ease of use drives good security; non-ease of use means people will write down passwords, which compromises both security and privacy, and violates HIPAA."

BEYOND HIPAA COMPLIANCE

While the current focus on improving security in healthcare is clearly being driven by the April 2005 HIPAA deadline, the advantages of ESSO extend beyond that initial need. With ESSO solutions such as On eSign, organizations can easily add cognitive security (strong passwords), token security (RSA SecureID, s wipe cards), and biometric security (retina scans, fingerprints). Once ESSO is deployed and in use, healthcare organizations can strengthen security further by adopting more stringent standards of their own.

For more details on OneSign, please visit: <http://www.imprivata.com> or contact Imprivata at: 877-ONESIGN.

Copyright © 2005 Imprivata, Inc.



10 Maguire Road Building 2 Lexington, MA 02421 v 781 674 2700 f 781 674 2760

1.877.ONESIGN

Imprivata Europe Forsyth House 77 Clarendon Road Watford Herts, WD17 1LE United Kingdom v+ 44 1923 813511 f +
44 1923 813501

www.imprivata.com