



OmniPass and HIPAA Compliance

WHITE PAPER

Disclaimer

This document is Copyright © 2002-2010 by Softex Inc. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided “as is” without any express or implied warranty.

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Softex or its partners. The listing of an organization does not imply any sort of endorsement and Softex takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Softex Inc., or any of Softex’s partners.

This document is for Education and Awareness Use Only

Introduction

The passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996 gave the federal government the ability to mandate the ways in which health care organizations store and transmit individuals' personal health information. Until HIPAA's passage, no national or industry standards governed the privacy and security of an individual's health information.

The HIPAA regulation has two parts that directly affect the information technology (IT) systems and software implemented by a healthcare organization: (1) The Privacy Rule and (2) The Security Rule.

The Privacy Rule

The purpose of the Privacy Rule is to establish minimum Federal standards for safeguarding the privacy of individually identifiable health information. Covered entities, which must comply with the Rule, include health plans, health care clearing houses, and certain health care providers.

The Rule confers certain rights on individuals, including rights to access and amend their health information and to obtain a record of when and why their Protected Health Information (PHI) has been shared with others for certain purposes.

The Security Rule

The HIPAA regulation also requires covered entities to take specific steps to protect Electronic PHI (ePHI). All security requirements can be defined as one of three basic safeguards: (1) administrative (2) physical and (3) technical. Some of the basic requirements are listed below and include, but are not limited to:

- Adopting policies and procedures to protect ePHI
- Adopting policies and procedures to protect the security of patient and enrollee information, including a policy on workstation use
- Developing and implementing data access control procedures
- Implement technical mechanisms to prevent unauthorized access
- Establish a reporting and response system for confidentiality violations

The HIPAA Privacy and Security Rule requirements are designed to be ubiquitous, technology neutral and scalable from the smallest of provider practices to the largest of health plans. Since many of the requirements of the Privacy and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of an exact template process, but rather a broad-based customized implementation based on a host of complex factors unique to each organization. This means that the IT systems and

software used in implementing compliance must be flexible, configurable, customizable and scalable so that the organization can fit the tools into existing processes to achieve compliance.

Meeting the Basic Security Rule Requirements

The HIPAA Security Rule requirements are broken down into three parts that cover all aspects of electronic PHI security and protection: (1) administrative safeguards (2) physical safeguards and (3) technical safeguards.

Administrative Safeguards

The administrative safeguards are actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce in relation to the protection of the information.

Physical Safeguards

Each covered entity is required to address the physical safeguard standards that concern the physical protection of data systems and data from intrusion and from environmental or natural hazards.

Technical Safeguards

The technical safeguard standards address the information technology protection, policies and procedures used to protect electronic PHI and control access to it. The following are included in the technical safeguards:

- **Person or Entity Authentication** – Covered entities must implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. For example, digital signatures, biometrics and soft tokens may be used to implement this standard.
- **Access Control** – Covered entities must implement technical policies and procedures for electronic information systems (computers) that maintain electronic PHI to allow access only to those persons or software programs that have been granted access as specified by the security safeguards. This standard requires the assignment of a unique name and/or number for identifying and tracking user identity, and establishing procedures for obtaining necessary electronic PHI during an emergency. Some facilities may wish to use encryption as a method of denying access to information in a file.
- **Transmission Security** – Covered entities must implement technical security measures to guard against unauthorized access to electronic

PHI that is being transmitted over an electronic communications network. Integrity controls, strong authentication and encryption are recommended to achieve this standard.

- **Integrity** – Covered entities must implement policies and procedures to protect electronic PHI from improper alteration or destruction. Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanism that are commonplace in hardware and operating systems today. Also, strong authentication of users that may modify electronic PHI can help with complying with integrity requirements.
- **Audit Controls** – Covered entities must implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. These are to be put in place to record and examine system activity.

OmniPass Product Family Overview

The OmniPass product family, which includes the OmniPass Client Edition and the OmniPass Enterprise Edition, can be used to help health care organizations protect electronic PHI as required by the HIPAA Security Rule. First, this whitepaper will present a brief overview of the OmniPass product, so that its applicability to the HIPAA Security Rule can be described later on.

The OmniPass family of products is the only comprehensive enterprise security solution available in the industry that can securely authenticate users and control access to computers, applications, and data. OmniPass can integrate with multiple types of authentication devices (such as biometric fingerprint readers, smart cards, contact-less badges, security chips, and tokens) and provide multi-factor authentication for Windows Logon security, authenticated sign-on to applications and websites (i.e. no more passwords) and secure file encryption, all integrated with Active Directory servers with IT administration capability.

The architecture of the OmniPass family supports broad ranging scalability and flexibility. The product family can be run in all environments from a client only, single user environment (like a small doctor's office) all the way up to a client / server, multi-user enterprise environment (like a large hospital or health plan). The OmniPass family is made of two primary components – the OmniPass Client Edition software that runs on the user's Windows based computer and the OmniPass Enterprise Edition server software that integrates the OmniPass clients with an enterprise's Active Directory or LDAP Server and provides back-end management of the environment by IT personnel.

The user interface of the OmniPass Client Edition is very user friendly and intuitive, thus making the secure computing experience easy to use for the enterprise user. This can greatly reduce the support burden on the corporate IT department during initial deployment, rollout and use of the OmniPass product family. The IT staff can administer OmniPass secured users and policies, machines, and devices from a simple administrator console based on the Microsoft Management Console (MMC) standard.

Figure 1 below outlines the wide ranging capabilities of the OmniPass Product Family. The figure is a summary of the features when the OmniPass Client Edition is used in conjunction with the OmniPass Enterprise Edition.

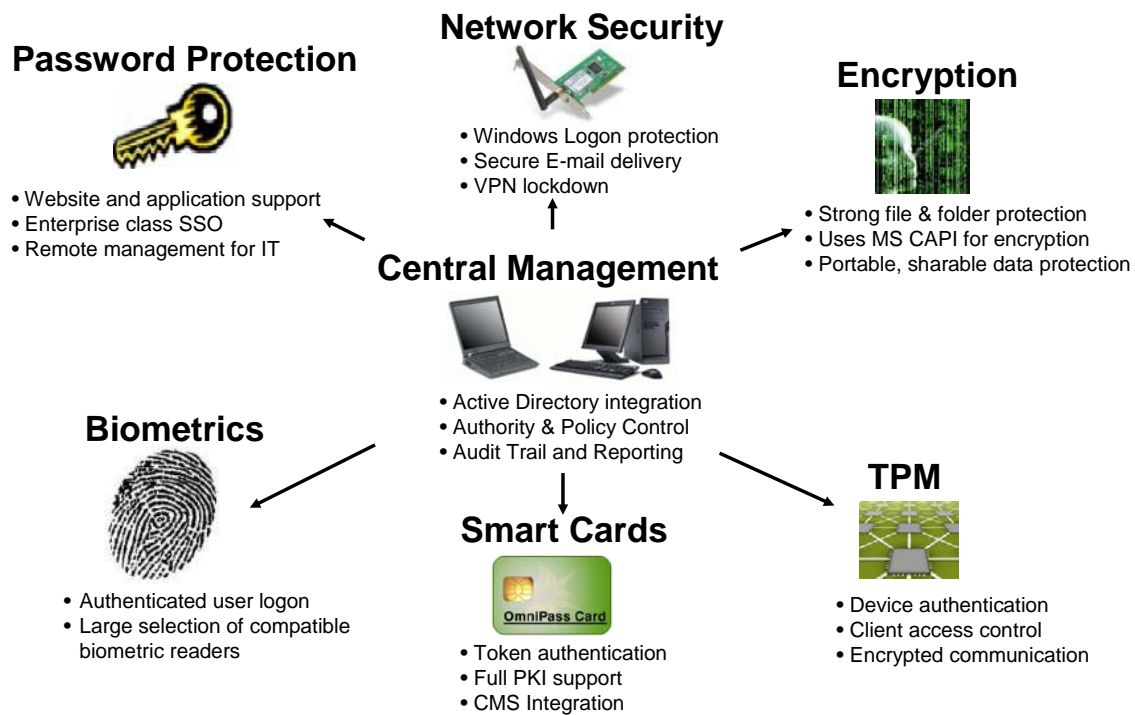


Figure 1. OmniPass Product Family Overview

Using OmniPass for HIPAA Compliance

A broad analysis of the HIPAA Security Rules requirements results in a set of common requirements to achieve compliance: (1) Strong user authentication for systems containing applications, files and other resources that handle electronic PHI, (2) securing and encrypting electronic PHI and (3) providing an audit and reporting trail for all access to electronic PHI. Of course, any IT manager will add

the implied requirement that any system put in place must be centrally manageable so that IT departments are not overburdened to deploy and maintain the technology.

The OmniPass Product Family implements all the necessary components for healthcare organizations to achieve strong HIPAA Security Rule compliance. OmniPass can be configured to use biometric devices, smart cards, contact-less badges, tokens or other devices to achieve strong multi-factor user authentication. OmniPass can force this authentication to log into a workstation containing electronic PHI and to access applications or websites containing sensitive patient data. OmniPass can also be used to encrypt electronic PHI and all accesses to the systems and applications containing sensitive data can be audited and reported as required by HIPAA. OmniPass can even be used to secure e-mail and other network transmission mechanisms that would be used to move electronic PHI between users in a healthcare organization.

OmniPass can also be easily deployed and managed by IT administrators in an enterprise environment. OmniPass provides a management console through which IT managers can setup user access policies for different applications and websites and encrypted data resources. IT administrators deploy the OmniPass Client Edition to all networked PCs using standard deployments tools and enrollment stations can be setup throughout an enterprise to facilitate easy enrollment of healthcare providers into the biometric reader, smart card or tokens device that will be used for strong authentication.

Figure 2 on the following page outlines some of the specific HIPAA Security Rule implementation requirements and how the OmniPass Product Family solution can address each to give strong HIPAA compliance.

HIPAA Security Rule Requirement	OmniPass Solution
Each user must be uniquely identified before being granted access to confidential information.	OmniPass provides flexible user authentication capabilities which support a range of methods, including biometrics, TPM, smart cards, and USB tokens. Methods can be combined for strong multifactor authentication.
Access to electronic PHI must be restricted to only those persons who need access as part of their role, and the conditions of this access must be clear.	OmniPass provides back-end management (via an easy to use management console) that is flexible with fine-grained policy management that helps control user's access to critical resources and information.
PHI must be reasonable safeguarded against intentional or inadvertent disclosure.	OmniPass can be used to setup centralized, policy-driven identity and access management that can be easily administered and that can enforce access to sensitive applications and data.
Access to protected resources must be tracked so that complete access reports can be generated.	OmniPass has comprehensive auditing and reporting capabilities that can track access to workstation, applications, websites and files that contain sensitive data.
Login attempts must be tracked so that suspicious login attempts can be analyzed and corrective action taken.	OmniPass can track logins both successful and unsuccessful login attempts and standard reporting tools can be used to analyze the data in real-time so that immediate corrective action can be taken.
Access to protected resources must be terminated quickly when an employee leaves the company.	OmniPass authentication is linked with Active Directory so if a user is removed from the AD, OmniPass will automatically fail all authentication requests for login, application and sensitive data access.
A user's session can be terminated after a specific period of inactivity.	OmniPass can be configured to automatically lock workstations or logoff users if the user removes his token, smart card or contact-less badge from the proximity of the workstation.
Procedures must be implemented for creating and managing passwords in the covered entity.	OmniPass can be used to replace all passwords in the environment with strong authentication such as a biometric swipe, smart card or token access. The cost and risk of passwords are completely eliminated for the covered entity.

Figure 2. HIPAA Security Rule Requirements and OmniPass Solutions

Conclusion

HIPAA compliance is an overall strategy and the OmniPass family is a powerful tool to implement that strategy. The OmniPass family of products is the only comprehensive enterprise security solution available in the industry that supports multiple authentication devices and multi-factor authentication for Windows logon security, single sign-on and file encryption all integrated with LDAP servers with IT administration capability. No other product in the industry integrates all the critical functions of logon security, password management and file encryption with security authentication devices.

OmniPass Enterprise Edition gives enterprises the scalability and flexibility to deploy and support any type of authentication technology and to manage user policy and settings, passwords, encryption information all centralized around corporate LDAP (Active Directory) servers.

References

Information for this document was derived from a NIST publication concerning HIPAA compliance. Additional documents used in preparation of this whitepaper are listed below:

National Institute of Standards and Technology (NIST):
<http://www.nist.gov>

SNIP Security and Privacy White Papers:
http://www.wedi.org/snip/public/articles/dis_publicDisplay.cfm?docType=6&wptype=2

Regional SNIP Efforts:
<http://www.wedi.org/snip/public/articles/index%7E2.htm>

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

About Softex

Founded in 1992, Softex has become a leading provider of computer security products and services. The OmniPass Client Edition is the industry's most widely deployed biometric client solution and is available or recommended for use with biometrically enabled devices from Lenovo, Fujitsu, Toshiba, Samsung, Medion, LG Electronics, and others as well as many peripheral vendors such as American Power Conversion, Targus, Fellowes, Hyundai Information Technology and others. Softex has also been named as one of Inc. Magazine's "Top 500 Fastest Growing Private Companies" in the United States in the year 2000.

For Sales Information, Please Contact:

Softex, Inc.
9300 Jollyville Road, Suite 201
Austin, TX 78759 USA
(512) 452-8836 main
(512) 795-8702 fax
www.softexinc.com