HEALTHCARE PRIVACY REQUIREMENTS AND HP SECURITY TOOLS

Business white paper

Changes in healthcare regulations promise important cost reductions and privacy protection for patients. Healthcare providers today are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications.

Although this data sharing ability has streamlined and improved healthcare operations, these changes also impose new burdens, costs and risks on healthcare providers. The rise in the adoption rate of these technologies increases the potential for data breaches. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was implemented to help protect confidential patient information, and healthcare organizations are now faced with penalties including hefty fines for the unauthorized release of this information. Studies show that 85% of healthcare organizations have suffered breaches of patient information, with an average cost of $2 million each. Up to 77% of those breaches resulted from a lack of IT security systems, making data protection an obvious area for concern.[1]

But healthcare organizations must balance that concern with ensuring the ability for authorized users to access information quickly and easily in order to provide necessary health services. Security must not impede normal operations, as these are often life-and-death situations.

Table of contents

The Privacy Rule

The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule regulates how certain entities, called covered entities, use and disclose certain individually identifiable health information, called protected health information (PHI).[2] Among other provisions, the Privacy Rule:

- Gives patients more control over their health information
- Sets boundaries on the use and release of health records
- Establishes appropriate safeguards that healthcare providers and others must achieve to protect the privacy of health information
- Holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights
- Generally limits release of information to the minimum reasonably needed for the purpose of the disclosure

The Security Rule

While the Privacy Rule pertains to all Protected Health Information including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). The Security Rule under HIPAA sets up a methodology that permits appropriate access to PHI, yet protects electronic PHI from unauthorized viewing.

Confidentiality, integrity, and availability of electronic protected health information (e-PHI) are the core principles of security. Transmissions of PHI over the Internet, extranet, leased lines, dial-up lines and private networks are all included. Security is defined as: Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.[3]

HITECH

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act took effect. The HITECH Act seeks to streamline healthcare and reduce costs through the use of health information technology, including the adoption of electronic health records. The Act widens the scope of privacy and security protections available under HIPAA, increases potential legal liability for non-compliance, and provides more enforcement of HIPAA rules.

HITECH requires healthcare organizations to take more responsibility for protecting patient records and health information. The provisions of the HITECH Act are specifically designed to work together to provide the necessary assistance and technical support to providers, enable coordination and alignment within and among states, establish connectivity to the public health community in case of emergencies, and assure the workforce is properly trained and equipped to be meaningful users of EHRs. Combined, these programs build the foundation for every American to benefit from an electronic health record, as part of a modernized, interconnected, and vastly improved system of care delivery.[4]

Meeting HIPAA and HITECH Requirements

The Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards: administrative, physical, and technical. Required specifications must be adopted and administered as dictated by the Security Rule. Addressable specifications are more flexible. Individual covered entities must evaluate their own situation and determine to implement the addressable specification or document why doing so would not be reasonable and appropriate and then implement an equivalent alternative measure.

- **Administrative safeguards**
  Administrative safeguards are administrative actions, policies and procedures put in place to manage the selection, development, implementation and maintenance of security measures to protect e-PHI, and to manage the conduct of the provider. Administrative safeguards mandate the development and implementation of policies and procedures that are focused on reasonable and appropriate access to, and protection of, e-PHI. These policies and procedures are designed to assist the entity with the acts' requirements.
- **Physical safeguards**
  Physical safeguards are the physical measures, policies and procedures put in place to protect a CE's electronic information system and the related buildings and equipment from unauthorized intrusion. This includes controlling physical access to hardware, as well as the introduction and removal of hardware, to protect against inappropriate access to protected data. For example, policies are required to address proper workstation use, including physical access to devices that are used to process or store PHI.

- **Technical safeguards**
  Technical safeguards cover technology and any policies and procedures for its use that protect electronic health information, controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically from being intercepted by anyone other than the intended recipient. For example, employing encrypting to securely transmit PHI over the Internet.

HP Solutions for HIPAA and HITECH Mandate

As a leading provider of technology solutions to healthcare organizations, HP is ready to support the HIPAA and HITECH needs of healthcare organizations with comprehensive data security solutions. Many new and existing HP data protection technologies, including HP ProtectTools and HP DigitalPersona[5], already assist with the privacy requirements under these federal mandates.

HP ProtectTools Overview

The HP ProtectTools portfolio brings together the security technologies and features for HP notebook, desktop and workstation computers. With HP ProtectTools, users and administrators don't need to read multiple reference manuals or spend hours setting up security applications. The HP ProtectTools includes a family of business-level PC security products, services and features, including Credential Manager, Security Manager, TPM Embedded Security, drive encryption, file sanitizer and Computrace® Pro.

Credential Manager

Credential Manager provides an interface to manage identity, credential, and multi-factor authentication through the HP ProtectTools Security Manager. It protects access to laptops and desktops with broad, multi-factor authentication and single sign-on options.

TPM Embedded Security (ISV)

Embedded Security for HP ProtectTools is a hardware security chip, called the Trusted Platform Module (TPM) that integrates the core elements of trust into the subsystem. The TPM is bound to a single platform and is independent of all other platform components (such as processor, memory and operating system). The TPM uses a root key protected in silicon to enhance native Microsoft™ operating system file and folder encryption and lay the foundation for authentication of TPM-enabled PCs to the network. Administrators use the TPM Embedded Security tool to create and deploy role-based policies from a central console. They can deploy suitable security policies for each user "group" including how users log on, and recover or revoke credentials, all from a single control point. They can also retrofit legacy PCs that did not come with HP ProtectTools. The key features of this tool includes.

- Central Management: Set up policies that include full disk encryption, multi-factor authentication and more
- Access Recovery: Recover from emergencies—such as users that forget their passwords when their computers are locked—with pre-boot authentication
- Two Factor VPN Authentication: Provide more secure access to the corporate network with multi-factor authentication for VPN
- Enterprise Single Sign-on: Get full access to the computer and other resources with a single authentication
- Full Disk Encryption: Protect customer data and intellectual property with full disk encryption
- Secure Communications: Share information more safely with signature and encryption for e-mail and documents

HP ProtectTools Wave Systems' EMBASSY® Trust Suite

When used in conjunction with Wave Systems' EMBASSY Trust Suite, the HP Embedded Security solution enables more secure and seamless file storage and business transactions. The combined solution from Wave Systems and HP provides customers with stronger PC security that is easy to administer and use, by IT staff and end-users alike.

Drive encryption for HP ProtectTools

HP ProtectTools uses the best way possible to protect the information on your hard drive—full volume encryption using proven McAfee technology. Drive Encryption encodes all the information on a hard disk drive (HDD), helping to keep your business-critical information protected and unreadable to unauthorized users.

File Sanitizer for HP ProtectTools

File Sanitizer works to remove files that could be used to identify, contact or locate users. It permanently deletes files, folders and identity information from notebook PCs and desktops to help protect users' personal information.

Computrace® Pro for HP ProtectTools

Computrace Pro tracks lost or stolen notebooks and remotely deletes data they contain.

Central Management for HP ProtectTools using DigitalPersona[5]

DigitalPersona is HP's central management partner that allows HP ProtectTools to remotely control access management, data protection and increase the security of communications for the entire organization. It is primarily used to centrally manage HP ProtectTools. Easy to deploy, administer and use, DigitalPersona Pro also includes client software you can install on computers that did not have HP ProtectTools as preloaded software.

DigitalPersona offers two options to centrally manage HP ProtectTools, including web-based DigitalPersona Pro Workgroup for small and medium-size businesses, and Active Directory integration using DigitalPersona Pro Enterprise for large organizations with managed IT environments. Both options include applications such as Disk Encryption, Strong Authentication, Single Sign On (SSO), Digital Signature, and more.

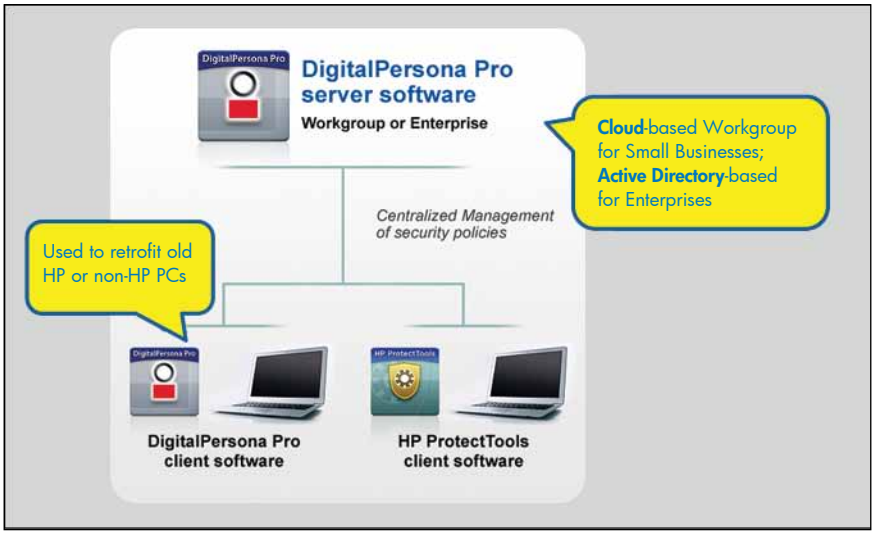

Figure 1. Components of HP ProtectTools

DigitalPersona Multi-Credential Authentication

Multi-credential authentication removes the need for traditional passwords that can be easily forgotten or exposed by paper trails or sticky notes, which could put healthcare organizations at risk for data breaches. This application utilizes a broad variety of mechanisms for multicredential authentication based on the optimal balance between security and convenience, including fingerprint biometrics, smart cards, face recognition, onetime password and Windows-password.

DigitalPersona Single Sign-On

Single Sign-On eliminates all passwords from staff's interactions with computing devices, thus streamlining workflow and removing the need to call IT. DigitalPersona's Single Sign-On enables single sign-on into an application without any changes to the application, and setup can be done in minutes.

DigitalPersona Authentication for PC and Kiosk Logon

Authentication for PC and Kiosk logon helps ensure secure access to shared computer stations while maintaining the convenience required to streamline staff access to critical patient information. It also enables tracking of who accessed which computer and when.

DigitalPersona Virtual Environment Access and Authentication

Healthcare staff can securely and easily logon to virtual environments, helping to ensure protected data exchange across computers.

DigitalPersona Full Disk Encryption

DigitalPersona Full Disk Encryption solutions rely on AES algorithms with strong 256-bit keys and multi-credential authentication to protect data in the event of a lost or stolen computer. It even protects data if a thief pulls out the hard drive and tries to access information using another computer.

DigitalPersona Digital Signature

Physicians and staff can rely on DigitalPersona's Digital Signature to improve accountability while increasing efficiency. The application enables electronic signature of prescriptions and other documents.

DigitalPersona Two Factor RADIUS Authentication

Security of existing Virtual Private Networks or other RADIUS applications (such as Citrix, Outlook Web Access, and others) can be improved by adding authentication based on one-time passwords and fingerprint or other desired authentication method.

DigitalPersona Email and Document Encryption

Users can share information more safely by encrypting email and documents.

DigitalPersona Cloud-Based Security Management

HP Secure Intranet Cloud Print

HP Secure Intranet Cloud Print can help with a more secure and assured delivery of electronic medical records and other business-critical information throughout the healthcare enterprise. It provides secure and reliable delivery, redundant and failover delivery processes and standards-based (SOA) programming integration with external applications based on XML, SOAP and WSDL technologies.

PC-based Security Tools

HP security products also include applications geared towards protecting individual PCs with HP fingerprint sensor, preboot security, drive encryption, privacy manager for protection of emails and instant messages and disk sanitizer.

HP Applications and the HIPAA and HITECH requirements

HP and its partner companies are dedicated to helping medical organizations satisfy the information privacy and access burdens imposed by federal and state regulations, while preserving their ability to provide excellent medical services whenever and wherever needed. This includes protecting confidential information, providing information to legitimate users, and speeding reimbursement for services rendered through easy integration with third-party payers.

Although HP's solutions address most of the technical requirements of the HIPAA and HITECH acts outlined in Table 1, the power can be seen most comprehensively in the following three key areas.

Password Management
HIPAA §164.308(a)(5)(ii)(D)

According to HIPAA, organizations should use "procedures for creating, changing and safeguarding passwords". A typical case might be the need to enforce the use of strong passwords to log on to enterprise medical applications.

DigitalPersona Pro[5] can help meet the requirements imposed by allowing IT managers to configure password management and Single Sign-on to all enterprise applications, or even randomize passwords, thus making it difficult to share credentials. With DigitalPersona Pro Enterprise, IT managers set up application logons through a simple wizard. Support extends to virtually all applications, such as Citrix®, Epic®, Meditech® and SAP®, as well as Web, Windows and terminal applications.

Implementation of Electronic Medical Records
HITECH §164.400–534

For medical practices looking for guidance in the transition to the "digital office," the HP EHReady program is an end-to-end solution designed to assist with HITECH criteria for meaningful use of electronic health records. EHReady is a comprehensive program that provides physicians with customized, end-to-end solutions of hardware, software, up-front support, installation, setup and training services. Specifically designed for the needs of any size medical office, this program suite offers a range of support, from consultation, planning and installation for PC, server, network and printing and scanning devices.
With HP Services, affiliated physicians can choose from the services that meet the exact needs for their office. Including:

- Onsite Assessment
- Implementation Design
- EHR Software & Hardware Integration
- Server, Network and Device Installation Services
- Fixed and Flexible Support Services
- Onsite & Remote Post Installation Support

Protecting Confidential Documents
HIPAA §164.308 and §164.312

HP Secure Intranet Cloud Print for Electronic Medical Records (EMR) is a software platform providing secure and assured delivery of EMR documents and other healthcare business-critical information throughout the healthcare enterprise. It provides secure and reliable document delivery. Including:

- Immediate alerts of output failures enabling corrective action, minimizing disruptions in patient care related to EMR output
- Automatic delivery re-tries and secure, audited re-routing, including job check pointing
- Centralized secure output management enabling simplified management of entire output infrastructure from the desktop to the datacenter
- Improved help desk support capabilities without compromising patient data
- Encrypted data from server to the device
- Secure printing capabilities

Mapping HIPAA/HITECH requirements to HP Solutions

In addition to the three specific examples featured above, many other HP security tools map easily into data protection requirements established by HIPAA and HITECH regulations. The following table shows how HP products correspond with several key areas of the new PHI protection regulations.

Table 1. HIPAA/HITECH requirements to HP Solutions[2,3,4,5]

HIPAA REGULATION	ID	HP SOLUTION
Administrative Safeguards	**§164.308**	
Security Management Process	(a)(1)(i) (a)(2)	• HP ProtectTools Security Manager • HP ProtectTools Embedded Security solution • DigitalPersona Coud-Based Security Management
Workforce Security	(a)(3)	• Log-in Monitoring • Password Management
Information Access Management	(a)(4)	• HP ProtectTools Security Manager • HP ProtectTools Embedded Security solution • DigitalPersona Multi-Credential Authentication • DigitalPersona Authentication for PC and Kiosk Logon • DigitalPersona Coud-Based Security Management • HP fingerprint sensor • HP Pre-boot security
Physical Safeguards	**§164.310**	
Access control and validation procedures **Workstation Use** **Workstation Security**	(a)(2)(iii) (b) (c)	• DigitalPersona Multi-Credential Authentication • DigitalPersona Single Sign-On • DigitalPersona Authentication for PC and Kiosk Logon • DigitalPersona Virtual Environment Access and Authentication • HP fingerprint sensor • HP Pre-boot security • HP ProtectTools Security Manager • DigitalPersona Multi-Credential Authentication • DigitalPersona Single Sign-On • DigitalPersona Authentication for PC and Kiosk Logon • DigitalPersona Virtual Environment Access and Authentication • Computrace® Pro for HP ProtectTools
Device and Media Controls **Disposal** **Media Reuse**	(d)(1) (d)(2)(i) (d)(2)(ii)	• HP drive encryption • Disk Sanitizer • File Sanitizer for HP ProtectTools • DigitalPersona Full Disk Encryption • Drive encryption for HP ProtectTools (ISV)
Data Backup and Storage	(d)(2)(iv)	• HP Backup and Restore • HP Sparekey • HP drive encryption • DigitalPersona Full Disk Encryption • Drive encryption for HP ProtectTools (ISV)
Technical Safeguards	**§164.312**	
Unique User Identification **Person or Entity Authentication**	(a)(2)(i) (d)	• DigitalPersona Multi-Credential Authentication • DigitalPersona Single Sign-On • DigitalPersona Authentication for PC and Kiosk Logon • DigitalPersona Virtual Environment Access and Authentication • HP fingerprint sensor • HP Pre-boot security • HP ProtectTools Security Manager • DigitalPersona Multi-Credential Authentication • DigitalPersona Single Sign-On • DigitalPersona Authentication for PC and Kiosk Logon • DigitalPersona Virtual Environment Access and Authentication • Computrace® Pro for HP ProtectTools
Encryption and Decryption	(a)(2)(iv)	• HP drive encryption • Disk Sanitizer • File Sanitizer for HP ProtectTools • DigitalPersona Full Disk Encryption • Drive encryption for HP ProtectTools (ISV) • DigitalPersona Email and Document Encryption
HITECH	**§164.400 534**	
Privacy of individually identifiable health information		• HP Secure Intranet Cloud Print for Electronic Medical Records (EMR) is a software platform SOAP and WSDL technologies • DigitalPersona Email and Document Encryption

HP Solutions for the Healthcare Industry

With a world of regulations already in place governing healthcare operations, the addition of HIPAA and HITECH rules often seem like an insurmountable added burden to many healthcare organizations. To add to that, long-standing practices and procedures for gathering, storing, and utilizing medical information often impede implementation, leading to fines that could threaten the financial health of healthcare institutions.

HP understands the challenges facing the healthcare industry. We bring nearly 40 years of experience in healthcare information technology and have worked with groups such as commercial healthcare plans, the U.S. Department of Defense Health Affairs, disease and care management organizations, Medicaid, and Medicare. HP is also intimately involved in developing e-commerce standards for the industry, and holds key positions with leading industry organizations. Including:

- Accredited Standards Committee (ASC) X12
- National Council for Prescription Drug Programs (NCPDP)
- Health Level 7 (HL7)
- Healthcare Information and Management Systems Society (HIMSS)
- Health Committee of the U.S. Chamber of Commerce
- American Accreditation HealthCare Commission/URAC
- Workgroup for ElectronicData Interchange (WEDI)

To Learn More

For more information about HP security solutions, contact your local HP representative to:

- Set up a workshop with HP to assess your specific HIPAA and HITECH needs
- Establish a plan to implement the best solution for today and into the future
- Identify an environmental approach that can help your company save money

Get the insider view on tech trends, alerts, and HP solutions for better business outcomes

1. The Ponemon Institute, available at http://www.itbusinessedge.com/slideshows/show.aspx?c=85046
2. US Department of Health and Human Services Health Information Privacy, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
3. US Department of Health and Human Services Health Information Privacy, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf
4. HITECH Act, available at http://www.hipaasurvivalguide.com/hitech-act-text.php
5. WP_Compliance_HIPAA_20100819[2], available at http://www.digitalpersona.com/resources/case-studies_white-papers/