



Health Insurance Portability & Accountability Act (HIPAA)



45 CFR: Health Insurance Reform Security Standards Final Rule

Information generated from a physical exam is no longer one just of medical diagnosis but one laden with regulation and process. When the digital age delivered efficiencies to the medical community, one of greater collaboration and access, new threats of data exposure became evident. The need to protect patient information from unauthorized access is now paramount throughout the U.S. as evidenced by enforceable HIPAA standards. This paper will focus upon the Security Standards Final Rule and explain how Digital Info Security Company's (DISC) email compliance and data security solution can help organizations with HIPAA compliance.

INDUSTRY CHALLENGE

Processing sensitive patient information requires the coordinated activities of multiple decentralized service organizations. Each organization handling a patient's Individually Identifiable Health Information (IIHI), whether by accessing it from a shared file server, transmitting it through email or backing-it-up to offline storage or removable media, must now adhere to new laws. Providers must ensure that the integrity, confidentiality and availability of the customer's data they collect, maintain, use and transmit is in fact protected in accordance with national standards set forth within the Health Insurance Portability and Accountability Act (HIPAA) of 1996¹.

HIPAA AND THE SECURITY STANDARDS FINAL RULE

The Health Insurance Portability Accountability Act of 1996 (HIPAA) is a multi-faceted regulation that addresses a variety of healthcare areas—from the portability of health insurance to information security and privacy. Privacy provisions were introduced, followed by security rules, to ensure the privacy of patient information and the security of systems.

The overall HIPAA privacy provisions became enforceable on April 14, 2003; however, it is the Security Standards Final Rule (referred to as "Final Rule" throughout the paper) that garners further attention. Published February 2003, the Final Rule specifies a series of administrative, technical, and physical security procedures to assure the confidentiality of electronic protected health information. Compliance for the initial implementation of the Final Rule was set for April 20, 2005, while small health plans had an extended compliance date of April 20, 2006.

While HIPAA's existing privacy provisions define what types of information has to be protected and under what circumstances, the Final Rule's security provisions define how that should be accomplished.

The following pages will outline the major sections of the Final Rule, highlight the technically-based components of each section and explain how the PolicyBridge™ II Suite with Magic KeyRing Security System™, an email compliance and data security solution from Digital Info Security Company (DISC), can help organizations with HIPAA compliance.

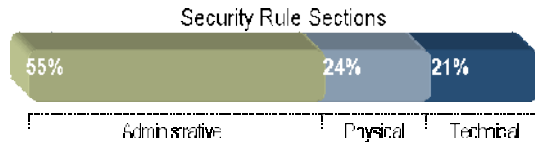
HIPAA encompasses a broad range of regulations that demand sweeping changes in the way healthcare companies operate. A universal remedy that single-handedly fulfills all the requirements that HIPAA encompasses is not proposed here. In fact, one should be leery of such a proposal due to the intricate and complex nature of the ruling.

¹ References: 45 CFR Sections 160, 162, 164: Health Insurance Reform: Security Standards; Final Rule. Available at <http://www.hhs.gov/ocr/hipaa>

MAJOR SECTIONS OF THE FINAL RULE

Appendix A of the Final Rule expands upon Title II of HIPAA. The matrix is broken down into three categories:

1. Administrative Safeguards – areas including security training, risk analysis and management, information access management, and security incident procedures. (45 CFR § 164.308)
2. Physical Safeguards – this section outlines requirements for protecting facilities and computer infrastructure (including workstations, devices and media) from unauthorized incursion and natural disasters. (45 CFR § 164.310)
3. Technical Safeguards – this section deals with encryption, authentication, transmission security, and other automated systems to protect and control access to actual data. (45 CFR § 164.312)



ADMINISTRATIVE SAFEGUARDS

Administrative Safeguards encompass the policies, procedures and documentation that describe how the organization is validating the security of the flow of information across the entire organization, thus demonstrating compliance.

PROCESS-BASED PROVISIONS

- Security management process
 - Risk analysis, management, sanction policy, and information system activity review
- Security awareness and training
- Assigned security responsibility
 - Required security officer or role
- Ongoing evaluation activities
- Business associate contracts

TECHNICAL-BASED PROVISIONS

Disaster contingency plan

Requires covered entities to establish and implement policies for responding to any event that results in the damage or loss of EPHI due to damage or loss of the systems and hardware on which it resides. In short, it necessitates the ability to create and maintain retrievable exact copies of EPHI.

∴ *Magic KeyRing Security System™ automatically captures, indexes, and archives all HIPAA-protected email and attachments, in their original form, for transfer to WORM media in offsite storage facilities.*

Workforce security

Directs organizations to implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI but prevent unauthorized employees from obtaining access to EPHI.

∴ *Magic KeyRing Security System's SecurWrap encryption with digital rights management and Security Manager provides the protection that only authorized users may gain access to sensitive data and additionally instills post data protection. If the status of an internal or external recipient of protected data changes, a single keystroke at the Security Server console instantly revokes access to secured content, whether selected content or all content, that has been delivered to that individual via email, network access or removable media. Anyone with whom the recipient may have been authorized to forward the EPHI to will also have access revoked. Magic KeyRing Security System™ automatically synchronizes with Active Directory via Lightweight Directory Access Protocol.*



Information access management

Calls for policies and procedures for granting access to EPHI either on workstations or through transactions, programs, processes or other mechanisms.

::: Magic KeyRing Security System™ aids in automating the enforcement of corporate policies and procedures due to its matrix of role, content and context-based access control

mechanisms that works directly with the protected patient data as it is stored or shared in email. For example, sensitive data can have (1) an expiration date can be applied; (2) persistent rights “wrapped²” with the data to control such activities as the ability to view, print, copy or forward. The creator of secured content can change permissions of wrapped data whether the individual is online, offline or acting as part of a clearinghouse, for example; and (3) if the status of an individual or group inside or outside the organization changes, access to any EPHI (regardless of where it resides) can be instantly expanded, limited or revoked from the centralized Magic KeyRing Security System™ Security Server.

“Security and privacy are inextricably linked. The protection of privacy of information depends in large part on the existence of security measures to protect that information.”

Department of Health and Human Services

Security incident procedures

Requires covered entities to identify and respond to suspected or known security violations, to mitigate any harmful consequences, when practical, and to document the incident and its outcome.

::: Magic KeyRing Security System™ can be an integral part of a covered entity’s overall security incident procedure with regard to EPHI that is stored or shared through email. It generates real-time security breach notifications and provides a full-text index to search and retrieve all activity and original information that matches its lexicon for forensic investigations.

PHYSICAL SAFEGUARDS

Physical safeguards are primarily concerned with facilities and hardware, such as:

- Facility access controls
- Workstation use
- Workstation security

Device and media controls

Concerns policies and procedures surrounding the receipt and removal of hardware and electronic media that contain EPHI so that the data is never compromised. The specification addresses activities about disposal, media reuse, accountability, and backup and storage that stipulate that media be cleared of EPHI before its disposal or reuse, that all movement of removable media be recorded and that an exact copy of EPHI be created before equipment is moved.

::: Magic KeyRing Security System™ offers three features that allow covered entities to conform to this provision. (1) When deleting data protected by Magic KeyRing Security System™, the remaining file structure is sanitized, whether the data was stored on a PC, file server, or removable media. (2) The tamper-resistant audit trail in Magic KeyRing Security System™ tracks all user activity, recording the movement of all data to electronic media and the person responsible therefore. (3) Magic KeyRing Security System™ automatically captures, indexes, and archives unaltered versions of all protected email and attachments.

² Wrapped data refers to the encryption technology from DISC. Encrypted data is protected in a self-contained encryption wrapper. This unique wrapper houses the set persistent rights information allowing off- and on-line access and auditing functionality.

TECHNICAL SAFEGUARDS

Technical safeguards outline the requirements of tools, solutions and system features that actually perform the work.

Access Control

Addresses the need to restrict access to EPHI only to those that have been so authorized. The standard requires the implementation of unique, traceable user identifications and when risk assessment deems appropriate, the use of encryption.

::: Magic KeyRing Security System™ ensures the unique identification of users through a single system-generated ID and password. It manages role, content, context and user-based access to sensitive information; defining permissions and strong encryption based on corporate HIPAA policies. Through encryption and granular levels of access control, Magic KeyRing Security System™ attaches security to sensitive data that persists after decryption. The software encapsulates EPHI in an encrypted wrapper either automatically, based on corporate policies, or manually, controlling permissions to Read, Write, Copy, Share (via email for example), Lock to Recipient PC or Time Expire.

Audit Controls

Requires covered entities to implement mechanisms that record and examine activity in systems that use EPHI.

::: Magic KeyRing Security System™ satisfies this condition by providing a tamper-resistant, time-stamped audit trail that tracks all users and all activities containing EPHI data.

Data Integrity

Urges covered entities to implement a system to authenticate electronic health information and corroborate that it has not been altered or destroyed in an unauthorized manner.

::: Magic KeyRing Security System™ can address this section of HIPAA by automatically identifying regulated information and wrapping it in an encrypted, rights managed container that ensures the contents cannot be altered. Easier to use than digital signatures, the Magic KeyRing Security System™ construct encrypts the actual data which means that alterations or deletions cannot occur without explicit authorization. Furthermore, any authorized changes are recorded in the time-stamped audit trail to ensure that authorized users are acting in accordance with their assigned level of authority.

Person or Entity Authentication

Task to verify that a person seeking access to EPHI is who he/she claims to be.

::: Magic KeyRing Security System™ can fulfill this demand because it uses a unique, system-generated username and password authentication system that can be adjusted to lock access to EPHI until the user re-authenticates with the Security Server for added identity verification.

Transmission Security

This section of the regulation specifically identifies encryption as a mechanism to employ, when deemed appropriate based on risk assessment, to ensure that EPHI is protected when transmitted over an electronic communications network.

::: Beyond simple encryption, Magic KeyRing Security System™ can exceed the recommended implementation of this provision by automatically applying protection measures to EPHI in transit through email. Based on HIPAA criteria, the software will block, quarantine, or encrypt email communications, and apply a permission wrapper to patient information before it moves beyond the network. The post delivery protection continues to enforce HIPAA policy, even after the information is received and decrypted.

FLEXIBLE DESIGN

The regulations are flexibly designed to accommodate the varying capabilities of large and small organizations to avoid undue financial burden on covered entities and by not being overly prescriptive to allow for technology advances. Accordingly, implementation specifications are designated as either “required” (non-negotiable) or “addressable.” If an implementation specification is addressable, then the organization must weigh whether it is a “reasonable and appropriate” precaution and determine the chosen methodologies it will implement given these factors:

- Size, complexity and capabilities of the covered entity
- Covered entity’s technical infrastructure, hardware, and software security capabilities
- Costs of security measures
- Probability and criticality of potential risks to EPHI³

WHO IS AFFECTED BY THE FINAL RULE?

The security implementation guidelines apply to all “covered entities” including medical providers, billing services, labs, and insurance companies. While HIPAA primarily applies to the healthcare sector, the privacy provisions and Final Rule affect other industries and businesses that have access to Electronically Protected Health Information (EPHI)—this means businesses that offer health insurance benefits packages.

Financial institutions are impacted by the Final Rule. In order to process HIPAA compliant payment transactions, financial institutions have to fulfill the same EPHI requirements as healthcare companies. Therefore, financial services clearinghouses that process or maintain healthcare information are subject to the Final Rule’s regulations.

ABOUT DIGITAL INFO SECURITY COMPANY (DISC)®

A leader in secure email compliance and data protection, DISC provides comprehensive solutions of email scanning with persistent policy management, compliance archival and auditing, and powerful encryption for email and company data. DISC solutions help enterprises with email compliance and protect themselves against intellectual property or business critical data leakage. DISC is headquartered in Westminster, CO, and is a publicly traded company under the symbol DGIF.



Digital Info Security Company
10030 CirclePoint Road, Suite 100
Westminster, CO 80020
866-841-5970
<http://www.disecurityco.com>

PolicyBridge™ II with Magic KeyRing Security System™ from DISC® is an integrated e-mail compliance and data protection solution that performs an integral part of a regulated entity’s overall secure internal controls system with regard to any financial information that is shared or stored. Magic KeyRing Security System™ includes SecurScan and SecurWrap.

SecurScan™ is an e-mail compliance tool that uses intelligent lexicon (customized to the financial sector) to identify regulated or compromising e-mail content. SecurScan can automatically enforce policies based on content, sender-receiver combinations, users, domains, and other criteria. E-mail and attachments can be blocked, returned to the sender, quarantined, routed to administrators or automatically protected by invoking the SecurWrap™ component.

SecurWrap™ is a proactive data protection tool that wraps sensitive information with user access control, time expiration policies and user action definitions such as read only, write, modify, delete, or forward. SecurWrap is able to protect spreadsheets, registration documents, prospectus documents, balance sheets, income statements, and any other SOX-regulated documents with persistent rights management protections. A tamper-resistant audit trail records all users who access or attempt to access protected content, all their activities with respect to that content and a time stamp of when the activity occurred to ensure that these critical documents are not altered or inappropriately attached to e-mail or saved to removable media.

SecurWrap can be automatically invoked during e-mail processing so that regulated documents or e-mails can be transmitted in a protected rights-managed wrapper, with permission rules that continue to enforce policy, even after delivery. Additionally, e-mail and attachments that meet policy criteria can be archived to comply with retention rules and for

³ Security 101 for Covered Entities, Available at <http://www.cms.hhs.gov/hipaa/hipaa2/education>