ITL Bulletin
ADVISING USERS ON INFORMATION TECHNOLOGY

IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE

By Joan S. Hash, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Introduction

To assist federal agencies with implementing the security standards required by the Health Insurance Portability and Accountability Act (HIPAA), NIST's Information Technology Laboratory released NIST Special Publication (SP) 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. This ITL Bulletin summarizes the special publication.

Background

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) defines security standards to be adopted for the protection of electronic protected health information (EPHI). These standards, known as the HIPAA Security Rule, were published by the Secretary of Health and Human Services (HHS) on February 20, 2003.

Purpose and Applicability

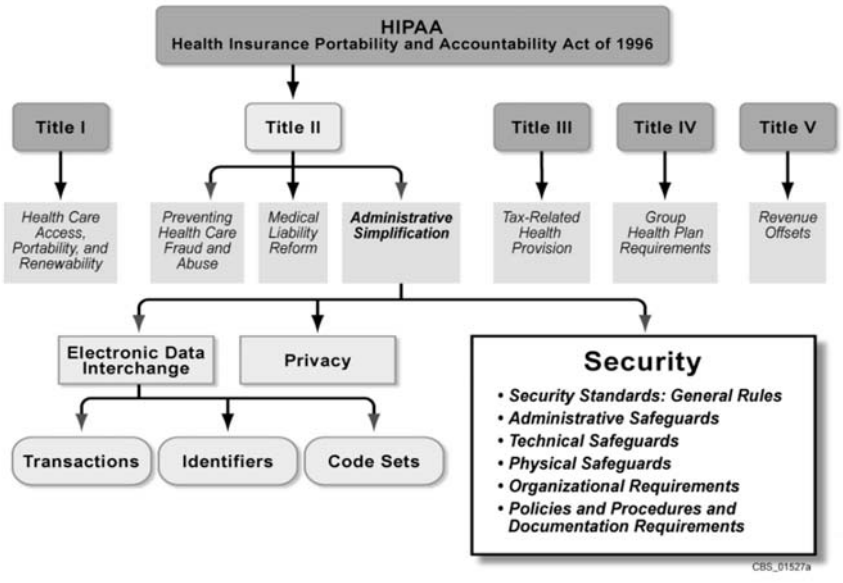
NIST SP 800-66 summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. The publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule.

Special Publication 800-66 is also designed to direct readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule. Readers can draw upon these publications for consideration in implementing the Security Rule.

Figure 1. shows all of the components of HIPAA and illustrates that the focus of NIST SP 800-66 is on the security provisions of the statute and the regulatory rule.

Continued on page 2

Figure1: HIPAA Components



ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since January 2004

"Covered entities" (except small health plans) must comply with the final Security Rule by April 21, 2005, and small health plans must comply by April 21, 2006.[1] Readers should refer to the Centers for Medicare and Medicaid Services (CMS) website, http://www.cms.hhs.gov/hipaa/hipaa2, for more detailed information about the passage of HIPAA by Congress, specific provisions of HIPAA, determination of the entities covered under the law, the complete text of the HIPAA Security Rule, the deadline for compliance with the Rule, and enforcement information.

The HIPAA Security Rule

The HIPAA Security Rule specifically focuses on the safeguarding of EPHI. Although the Federal Information Security Management Act (FISMA) applies to all federal agencies and all information types, only a subset of agencies is subject to the HIPAA Security Rule based on their functions and use of EPHI. All HIPAA covered entities, which includes some federal agencies, must comply with the Security Rule. The Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following covered entities:

- **Covered Health Care Providers—** Any provider of medical or other health services or supplies, who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- **Health Plans—** Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Health Care Clearinghouses—** A public or private entity that processes another entity's health care transactions from a standard format to a nonstandard format, or vice versa.
- **Medicare Prescription Drug Card Sponsors** – A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act. This fourth category of "covered entity" will remain in effect until the drug card program ends in 2006.

Security Rule Goals and Objectives

As required by the "Security standards: General rules"[2] section of the HIPAA Security Rule, each covered entity must:

- Ensure the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

Security Rule Organization

To understand the requirements of the HIPAA Security Rule, it is helpful to be familiar with the basic security terminology it uses to describe the security standards. By understanding the requirements and the terminology in the HIPAA Security Rule, it becomes easier to see which NIST publications may be appropriate reference resources and where to find more information. The Security Rule is separated into six main sections that each include several standards and implementation specifications a covered entity must address.[3] Each of the six sections is listed below.

- **Security standards: General Rules** includes the general requirements all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications (both required and addressable); outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information.
- **Administrative Safeguards** are defined in the Security Rule as the "administrative actions and policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- **Physical Safeguards** are defined as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- **Technical Safeguards** are defined as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

1. The definition of "small health plan" at 45 CFR § 160.103 applies to all of the HIPAA rules, including the Security Rule. A "small" health plan is one with annual receipts of $5 million or less.

2. See 45 C.F.R. § 164.306(a).

3. Sections of the HIPAA regulations that are included in the Security Rule and therefore addressed in this document but do not have their own modules are *Part 160 — General Administrative Requirements* § 160.103, *Definitions*; *Part 164 — Security and Privacy* §§ 164.103, *Definitions*; 164.104, *Applicability*; 164.105, *Organizational requirements* (discussed in section 4 of this document), 164.302 *Applicability*; 164.304, *Definitions*; 164.306, *Security standards: General rules* (discussed in section 3.1 of this document), and 164.318, *Compliance dates for the initial implementation of the security standards*.

Table 1: HIPAA Security Rule Standards and Implementation Specifications
Adapted from 68 Federal Register 8380, February 20, 2003 (Appendix A to Subpart C of Part 164--Security Standards: Matrix)

Standards	Sections	Implementation Specifications (R)=Required (A)=Addressable	
Administrative Safeguards			
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R)	Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	[None]	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)	
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions (R) Access Authorization (A) Access Establishment and Modification (A)	
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)	
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)	
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedures (A) Applications and Data Criticality Analysis A)	
Evaluation	164.308(a)(8)	[None]	
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)	
Physical Safeguards			
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)	
Workstation Use	164.310(b)	[None]	
Workstation Security	164.310(c)	[None]	
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R)	Accountability (A) Data Backup and Storage (A)
Technical Safeguards			
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R)	Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	[None]	
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	
Person or Entity Authentication	164.312(d)	[None]	
Transmission Security	164.312(e)(1)	Integrity Controls (A)	Encryption (A)

- **Organizational Requirements** includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations, and requirements for group health plans.
- **Policies and Procedures and Documentation Requirements** requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

Within the Security Rule sections are standards and implementation specifications. Each HIPAA Security Rule standard is required. A covered entity is required to comply with all standards of the Security Rule with respect to all EPHI. Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard.[4] Implementation specifications are either required or addressable. However, regardless of whether a standard includes implemen-

4. For more information on the required analysis used to determine the manner of implementation of an implementation specification, see § 164.306(d) of the HIPAA Security Rule (Security standards — General rules: Flexibility of approach).

tation specifications, covered entities must comply with each standard.

- A *required* implementation specification is similar to a standard, in that a covered entity must comply with it.
- For *addressable* implementation specifications, covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment.

Conclusion

NIST SP 800-66 includes both a mapping of the HIPAA Security Rule standards to supporting NIST publications, which can be used to assist with the HIPAA Security Rule implementation, and a mapping of HIPAA requirements to the Federal Information Security Management Act (FISMA) requirements. It is a valuable resource for federal agencies subject to compliance with both pieces of legislation. The document is available at http://csrc.nist.gov/publications/nistpubs/index.html.

***Disclaimer**: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.*

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195