HIPAA Security
SERIES

Security Topics

1 Security 101 for Covered Entities

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "Security Standards for the Protection of Electronic Protected Health Information", found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule, and assistance with implementation of the security standards. While there is no one approach that will guarantee successful implementation of all the security standards, this series aims to explain specific requirements, the thought process behind those requirements, and possible ways to address the provisions. This first paper in the series provides an overview of the Security Rule and its intersection with the HIPAA Privacy Rule, the provisions of which are at 45 CFR Part 160 and Part 164, Subparts A and E.

Compliance Deadlines

No later than April 20, 2005 for all covered entities except small health plans which have until no later than April 20, 2006.

Administrative Simplification

Congress passed the Administrative Simplification provisions of HIPAA, among other things, to protect the privacy and security of certain health information, and promote efficiency in the health care industry through the use of standardized electronic transactions.

The health care industry is working to meet these challenging goals through successful implementation of the Administrative Simplification provisions of HIPAA. The Department of Health and Human Services (HHS) has published rules implementing a number of provisions, including:

Security Regulation

The final Security Rule can be viewed and downloaded from the CMS Website at:
http://www.cms.hhs.gov/hipaa/hipaa2

■ **Privacy Rule** – The deadline for compliance with privacy requirements that govern the use and disclosure of protected health information (PHI) was April 14, 2003, except for small health plans which had an April 14, 2004 deadline. (Protected health information, or "PHI", is defined at 45 CFR § 160.103, which can be found on the OCR website at http://hhs.gov/ocr/hipaa.)

■ **Electronic Transactions and Code Sets Rule** – All covered entities should have been in compliance with the electronic transactions and code sets standard formats as of October 16, 2003.

■ **National identifier requirements for employers, providers, and health plans -** The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers. Covered entities must use this identifier effective July 30, 2004 (except for small health plans, which have until August 1, 2005). The National Provider Identifier (NPI) was adopted as the standard unique health identifier for health care providers. The Final Rule becomes effective May 23, 2005. Providers may apply for NPIs on or after that date. The NPI compliance date for all covered entities, except small health plans, is May 23, 2007; the compliance date for small health plans is May 23, 2008. The health plan identifier rule is expected in the coming years.

■ **Security Rule -** All covered entities must be in compliance with the Security Rule no later than April 20, 2005, except small health plans which must comply no later than April 20, 2006. The provisions of the Security Rule apply to electronic protected health information (EPHI).

Who must comply?

All HIPAA covered entities must comply with the Security Rule. In general, the standards, requirements, and implementation specifications of HIPAA apply to the following covered entities:

■ **Covered Health Care Providers -** Any provider of medical or other health care 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 health 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 non-standard 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.

For more information on who is a covered entity under HIPAA, visit the Office for Civil Rights (OCR) website at www.hhs.gov/ocr/hipaa or the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2. An online tool to determine whether an organization is a covered entity is available on the CMS website, along with a number of frequently asked questions (FAQs).

Why Security?

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of computers to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions. For example, in order to provide more efficient access to critical health information, covered entities are using web-based applications and other "portals" that give physicians, nurses, medical staff as well as administrative employees more access to electronic health information. Providers are also 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. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from

HIPAA SECURITY

Confidentiality -
EPHI is accessible only by authorized people and processes

Integrity -
EPHI is not altered or destroyed in an unauthorized manner

Availability -
EPHI can be accessed as needed by an authorized person

NOTE: Security is not a one-time project, but rather an on-going, dynamic process that will create new challenges as covered entities' organizations and technologies change.

wherever they are), the rise in the adoption rate of these technologies creates an increase in potential security risks.

As the country moves towards its goal of a National Health Information Infrastructure (NHII), and greater use of electronic health records, protecting the confidentiality, integrity, and availability of EPHI becomes even more critical. The security standards in HIPAA were developed for two primary purposes. First, and foremost, the implementation of appropriate security safeguards protects certain electronic health care information that may be at risk. Second, protecting an individual's health information, while permitting the appropriate access and use of that information, ultimately promotes the use of electronic health information in the industry – an important goal of HIPAA.

The Privacy Rule and Security Rule Compared

The Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access. With the passing of both the privacy and the electronic transactions and code set standards compliance deadlines, many covered entities are focusing on the security requirements. In developing the Security Rule, HHS chose to closely reflect the requirements of the final Privacy Rule. The Privacy Rule requires covered entities to have in place appropriate administrative, physical, and technical safeguards and to implement those safeguards reasonably. As a result, covered entities that have implemented the Privacy Rule requirements in their organizations may find that they have already taken some of the measures necessary to comply with the Security Rule. The primary distinctions between the two rules follow:

> **NOTE:** The Security Rule applies only to EPHI, while the Privacy Rule applies to PHI which may be in electronic, oral, and paper form.

- ■ **Electronic vs. oral and paper:** It is important to note that the Privacy Rule applies to all forms of patients' protected health information, whether electronic, written, or oral. In contrast, the Security Rule covers only protected health information that is in electronic form. This includes EPHI that is created, received, maintained or transmitted. For example, EPHI may be transmitted over the Internet, stored on a computer, a CD, a disk, magnetic tape, or other related means. The Security Rule does not cover PHI that is transmitted or stored on paper or provided orally.

- ■ **"Safeguard" requirement in Privacy Rule:** The Privacy Rule contains provisions at 45 CFR § 164.530(c) that currently require covered entities to adopt certain safeguards for PHI. While compliance with the Security Rule is not required until 2005 for most entities (2006 for small health plans), the actions covered entities took to implement the Privacy Rule may already address some Security requirements. Specifically, 45 CFR § 164.530 (c) of the Privacy Rule states:

> **NOTE:** OCR within HHS oversees and enforces the Privacy Rule, while CMS oversees and enforces all other Administrative Simplification requirements, including the Security Rule.

(c)(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

> *(2) Implementation specification: safeguards.*
> *(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.*
>
> *(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.*

■ The Security Rule provides for far more comprehensive security requirements than 45 CFR § 164.530 (c) of the Privacy Rule and includes a level of detail not provided in that section. As covered entities begin security compliance planning initiatives, they should consider conducting an assessment of the initiatives implemented for privacy compliance.

> **NOTE:** State laws that are contrary to the Privacy Rule and Security Rule are preempted by the Federal requirements, unless a specific exception applies. For more information, see 45 C.F.R. Part 160, Subpart B.

Implementation Specifications

An "implementation specification" is an additional detailed instruction for implementing a particular standard. Each set of safeguards is comprised of a number of standards, which, in turn, are generally comprised of a number of implementation specifications that are either required or addressable. If an implementation specification is required, the covered entity must implement policies and/or procedures that meet what the implementation specification requires. If an implementation specification is addressable, then the covered entity must assess whether it is a reasonable and appropriate safeguard in the entity's environment. This involves analyzing the specification in reference to the likelihood of protecting the entity's EPHI from reasonably anticipated threats and hazards. If the covered entity chooses not to implement an addressable specification based on its assessment, it must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure. See C.F.R. § 164.306(d)(ii)(B)(2) for more information.

> **NOTE:**
> Implementation specifications in the Security Rule are either "Required" or "Addressable". See 45 C.F.R. § 164.306(d).

For each of the addressable implementation specifications, a covered entity must do one of the following:

■ Implement the specification if reasonable and appropriate; or

■ If implementing the specification is not reasonable and appropriate –

- Document the rationale supporting the decision and

- Implement an equivalent measure that is reasonable and appropriate and that would accomplish the same purpose or

- Not implement the addressable implementation specification or an equivalent alternative measure, if the standard could still be met and implementing the specification or an alternative would not be reasonable or appropriate.

If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must consider options for implementing it. The decision regarding which security measures to implement to address the standards and implementation specifications will depend on a variety of factors, including:

■ **The entity's risk analysis –** What current circumstances leave the entity open to unauthorized access and disclosure of EPHI?

■ **The entity's security analysis -** What security measures are already in place or could reasonably be put into place?

NOTE: For more information about Risk Analysis, see paper 6 in this series, "Basics of Risk Analysis and Risk Management."

■ **The entity's financial analysis -** How much will implementation cost?

Overview of the Process

The table of required and addressable implementation specifications included in this paper outlines the standards and implementation specifications in the Security Rule. In order to comply with the Security Rule, all covered entities should use the same basic approach. The process should, at a minimum, require covered entities to:

■ **Assess current security, risks, and gaps.**

■ **Develop an implementation plan.**

- **Read the Security Rule.** A covered entity should review all the standards and implementation specifications. The matrix at the end of the Security Rule is an excellent resource when developing an implementation plan, and is included at the end of this paper.

- **Review the addressable implementation specifications.** For each addressable implementation specification, a covered entity must determine if the implementation specification is reasonable and appropriate in its environment. A covered entity needs to consider a number of factors in making the decisions for each addressable implementation specification.

- **Determine security measures.** A covered entity may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications. (See 45 CFR § 164.306(b), Flexibility of approach)

■ **Implement solutions.** A covered entity must implement security measures and solutions that are reasonable and appropriate for the organization.

■ **Document decisions.** A covered entity must document its analysis, decisions and the rationale for its decisions.

> **NOTE:** The Security Rule requires that a covered entity document the rationale for many of its security decisions.

■ **Reassess periodically.** A covered entity must periodically review and update its security measures and documentation in response to environmental and operational changes that affect security of its EPHI.

Flexible and scalable standards

The security requirements were designed to be technology neutral and scalable from the very largest of health plans to the very smallest of provider practices. Covered entities will find that compliance with the Security Rule will require an evaluation of what security measures are currently in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of complex factors unique to each organization.

HHS recognizes that each covered entity is unique and varies in size and resources, and that there is no totally secure system.

> **From 45 CFR § 164.306(b): Factors that must be considered -**
>
> - The size, complexity and capabilities of the covered entity.
> - The covered entity's technical infrastructure, hardware, and software security capabilities.
> - The costs of security measures.
> - The probability and criticality of potential risks to EPHI.

Therefore, the security standards were designed to provide guidelines to all types of covered entities, while affording them flexibility regarding how to implement the standards. Covered entities may use appropriate security measures that enable them to reasonably implement a standard. In deciding which security measures to use, a covered entity should take into account its size, capabilities, the costs of the specific security measures and the operational impact.

For example, covered entities will be expected to balance the risks of inappropriate use or disclosure of EPHI against the impact of various protective measures. This means that smaller and less sophisticated practices may not be able to implement security in the same manner and at the same cost as large, complex entities. However, cost alone is not an acceptable reason to not implement a procedure or measure.

Technology Neutral Standards

> **NOTE:** The security standards do not dictate or specify the use of specific technologies.

Over the last few years, the emergence of new technologies has driven many health care initiatives. With technology improvements and rapid growth in the health care industry, the need for flexible, technology-neutral standards is critical to successful implementation. When the final Security Rule was published, the security standards were designed to be "technology neutral" to accommodate changes. The rule does not prescribe the use of specific technologies, so that the health care community will not be bound by specific systems and/or software that may become obsolete. HHS also recognizes that the security needs of covered entities can vary significantly. This flexibility within the rule enables each entity to choose technologies to best meet its specific needs and comply with the standards.

Security Standards

The security standards are divided into the categories of administrative, physical, and technical safeguards. Regulatory definitions of the safeguards can be found in the Security Rule at 45 CFR § 164.304.

- **Administrative safeguards**: In general, these are the administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual and security training requirements. (For more information, see 45 CFR § 164.308 and paper 2 of this series titled "Security Standards – Administrative Safeguards".)

- **Physical safeguards:** In general, these are the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion. They include restricting access to EPHI and retaining off site computer backups. (For more information, see 45 CFR § 164.310 and paper 3 "Security Standards – Physical Safeguards".)

- **Technical safeguards:** In general, these are primarily the automated processes used to protect data and control access to data. They include using

authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being stored and/or transmitted. (For more information, see 45 CFR § 164.312 and paper 4 "Security Standards – Technical Safeguards".)

A complete list of the administrative, physical, and technical safeguards and their required and addressable implementation specifications is included at the end of this paper. In addition to the safeguards, the Security Rule also contains several standards and implementation specifications that address organizational requirements, as well as policies and procedures and documentation requirements. (See 45 CFR § 164.314 and § 164.316 of the Security Rule.)

Resources

The remaining papers in this series will address specific topics related to the Security Rule. Covered entities should periodically check the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2 for additional information and resources as they work through the security implementation process. There are many other sources of information available on the Internet. Covered entities may also want to check with other local and national professional health care organizations, such as national provider and health plan associations.

Need more information?

Visit the CMS website often at http://www.cms.hhs.gov/hipaa/hipaa2 for the latest security papers, checklists, webcasts, and announcements of upcoming events.

Call the CMS HIPAA Hotline at 1-866-282-0659, use the HIPAA TTY 877-326-1166, or email CMS at askhipaa@cms.hhs.gov

Visit the Office for Civil Rights website, http://www.hhs.gov/ocr/hipaa, for the latest guidance, FAQs, white papers and other information on the Privacy Rule.

Security Standards Matrix (Appendix A of the Security Rule)

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
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)		**(R)**
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)		**(R)**
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	**(R)**

PHYSICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications** **(R)= Required, (A)=Addressable**	
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)		**(R)**
Workstation Security	164.310(c)		**(R)**
Device and Media Controls	164.310(d)(1)	Disposal	**(R)**
		Media Re-use	**(R)**
		Accountability	**(A)**
		Data Backup and Storage	**(A)**
TECHNICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications** **(R)= Required, (A)=Addressable**	
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)		**(R)**
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	**(A)**
Person or Entity Authentication	164.312(d)		**(R)**
Transmission Security	164.312(e)(1)	Integrity Controls	**(A)**
		Encryption	**(A)**