HIPAA Security SERIES

Security Topics

1. Security 101 for Covered Entities
2. Security Standards - Administrative Safeguards
3. Security Standards - Physical Safeguards
4. Security Standards - Technical Safeguards
5. ★ Security Standards - Organizational, Policies and Procedures and Documentation Requirements
6. Basics of Risk Analysis and Risk Management
7. Implementation for the Small Provider

5 Security Standards: Organizational, Policies and Procedures and Documentation Requirements

What is the Security Series?

The security series of papers provides 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. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

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.

CMS recommends that covered entities read the first paper in this series, "Security 101 for Covered Entities" before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This fifth paper in the series is devoted to the standards for Organizational Requirements and Policies and Procedures and Documentation Requirements, and their implementation specifications, and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, "Security 101 for Covered Entities," visit the CMS website at: ***www.cms.hhs.gov/SecurityStandard/*** under the "Regulation" page.

Background

Three earlier papers in this series discuss the Administrative, Physical, and Technical Safeguards standards in the Security Rule. While these

HIPAA SECURITY STANDARDS

Security Standards: General Rules

ADMINISTRATIVE SAFEGUARDS
- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

PHYSICAL SAFEGUARDS
- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

TECHNICAL SAFEGUARDS
- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

ORGANIZATIONAL REQUIREMENTS
- Business Associate Contracts or Other Arrangements
- Requirements for Group Health Plans

POLICIES and PROCEDURES and DOCUMENTATION REQUIREMENTS

safeguards comprise the vast majority of standards and implementation specifications, there are four other standards that must be implemented; the other four standards are addressed in this paper and in 45 CFR §§ 164.314 and 164.316.

The standards at 45 CFR § 164.314, Organizational Requirements, and § 164.316, Policies and Procedures and Documentation Requirements, immediately follow the Technical Safeguards standards. They are not included in Appendix A the "Security Standards: Matrix" that is found at the end of the Security Rule, but must not be overlooked by covered entities. These requirements must be implemented to achieve compliance.

The objectives of this paper are to:

- Review each Organizational Requirements and Policies and Procedures and Documentation Requirements standard and implementation specification listed in the Security Rule.
- Discuss the purpose for each standard.

§ 164.314 - Organizational Requirements

STANDARD § 164.314(a)(1) — Business Associate Contracts or Other Arrangements

The Business Associate Contracts and Other Arrangements standard found at § 164.308(b)(1) requires a covered entity to have contracts or other arrangements with business associates that will have access to the covered entity's electronic protected health information (EPHI). The standard, at § 164.314(a)(1), provides the specific criteria required for written contracts or other arrangements between a covered entity and its business associates. The actual language used to address the requirements can be tailored to the needs of each organization, as long as the requirements are addressed.

In general, a business associate is a person or entity other than a member of the covered entity's workforce that performs functions or activities on the covered entity's behalf, or provides specified services to the covered entity, that involve the use or disclosure of protected health information. A business associate may also be a covered entity.

For example, a health care clearinghouse may be a business associate and is also a covered entity under HIPAA. A software vendor may be a business associate as well; however, it is not, in that capacity, a covered entity. In both cases, the organizations could perform certain functions, activities or services on behalf of the covered entity and would therefore be business associates. (See 45 CFR § 160.103, for the definition of "business associate.")

Section 164.314(a)(1)(ii) also identifies certain situations when a covered entity would not be in compliance with this standard despite the existence of a business associate contract.

> *"(ii) A covered entity is not in compliance with the standards in § 164.502(e) [the HIPAA Privacy Rule - Disclosures to Business Associates standard] and paragraph (a) of this section [the Business Associate Contracts or Other Arrangements standard] if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful –*
>
> *(A) Terminated the contract or arrangement, if feasible; or*
> *(B) If termination is not feasible, reported the problem to the Secretary."*

The two implementation specifications of this standard are:

1. Business associate contracts (Required)
2. Other arrangements (Required)

1. BUSINESS ASSOCIATE CONTRACTS (R) – *§ 164.314(a)(2)(i)*

The Business Associate Contracts implementation specifications state that a business associate contract must provide that the business associate will:

> *"(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity…;*
>
> *(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;*

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract."

Covered entities may already have business associate contracts in place in order to comply with the Privacy Rule. If the business associate creates, receives, maintains, or transmits EPHI, these existing contracts should be reviewed and modified in order to meet the Security Rule Business Associate Contracts requirements. Alternatively, covered entities could have two separate contracts to address the requirements of the Privacy and Security Rules respectively.

2. OTHER ARRANGEMENTS (R) - *§ 164.314(a)(2)(ii)*

The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract. If statutory obligations of the covered entity or its business associate do not permit the covered entity to include in its other arrangements authorization of the termination of the contract by the covered entity, the termination authorization may be omitted. (See §164.314(a)(2)(ii)(C).)

This implementation specification also applies to certain situations in which other laws require a business associate to perform certain functions or activities on behalf of the covered entity or provide certain services to the covered entity. These situations will not be discussed in detail within this paper. (See § 164.314(a)(2)(ii)(B).)

STANDARD § 164.314(b)(1) Requirements for Group Health Plans

The second standard in § 164.314 is the Requirements for Group Health Plans. The standard requires a group health plan to ensure that its plan documents require the plan sponsor to reasonably and appropriately safeguard EPHI that it creates, receives, maintains or transmits on behalf of the group health plan. (See 45 CFR § 164.314(b)(1).) Specific exceptions to this requirement are provided when the only EPHI disclosed to a plan sponsor is disclosed pursuant to permitted disclosures under the HIPAA Privacy Rule, specifically § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508. The standard includes the following required implementation specifications:

NOTE: The definition of a Group Health Plan can be found in 45 CFR § 160.103.

IMPLEMENTATION SPECIFICATIONS - § 164.314(b)(2)

The plan documents of the group health plan must incorporate provisions to require the plan sponsor to:

"(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) [of the Privacy Rule] is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware."

In other words, the Security Rule generally requires that if the plan sponsor of a group health plan has access to EPHI beyond summary information and enrollment information or to EPHI other than that which has been authorized under § 164.508, the plan documents must contain language similar to that already required by the Privacy Rule.

§ 164.316 – Policies and procedures and documentation requirements

In addition to the policies, procedures and documentation contained throughout the Security Rule, § 164.316 sets forth specific requirements for all policies, procedures and documentation required by the Rule.

STANDARD § 164.316(a) Policies and Procedures

The first standard, Policies and Procedures, contains several important concepts. Specifically, it requires that covered entities:

> *"Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart."*

The reference to § 164.306(b)(2), the Security Standards: General Rules, is specifically to the "Flexibility of Approach" provisions that outline the types of factors covered entities must consider when implementing the Security Rule.

NOTE: For more information about the concepts behind the General Standards, see the first paper in this series, "Security 101 for Covered Entities."

While this standard requires covered entities to implement policies and procedures, the Security Rule does not define either "policy" or "procedure." Generally, policies define an organization's approach. For example, most business policies establish measurable objectives and expectations for the workforce, assign responsibility for decision-making, and define enforcement and consequences for violations. Procedures describe how the organization carries out that approach, setting forth explicit, step-by-step instructions that implement the organization's policies.

Policies and procedures should reflect the mission and culture of the organization; thus, the Security Rule enables each covered entity to use current standard business practices for policy development and implementation. Polices and procedures required by the Security Rule may be

modified as necessary to meet the changing needs of the organization, as long as the changes are documented and implemented in accordance with the Security Rule.

The Policies and Procedures standard is further explained and supported by the Documentation standard.

STANDARD § 164.316(b)(1) Documentation

The Documentation standard requires covered entities to:

> *"(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."*

The Documentation standard has three implementation specifications.

1. Time Limit (Required)
2. Availability (Required)
3. Updates (Required)

1. TIME LIMIT (R) - *§ 164.316(b)(2)(i)*

The Time Limit implementation specification requires covered entities to:

> *"Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later."*

This six-year period must be considered the minimum retention period for required documentation under the Security Rule. Some organizations may choose to keep their documentation longer based on state law, requirements of accreditation organizations, or other business reasons.

2. AVAILABILITY (R) - *§ 164.316(b)(2)(ii)*

The Availability implementation specification requires covered entities to:

> *"Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."*

Organizations often make documentation available in printed manuals and/or on Intranet websites.

3. UPDATES (R) - *§ 164.316(b)(2)(iii)*

The Updates implementation specification requires covered entities to:

> *"Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."*

The need for review and update will vary based on a covered entity's documentation review frequency and/or the volume of environmental or operational changes that affect the security of EPHI. This implementation specification requires covered entities to manage their documentation so that it reflects the current status of their security plans and procedures implemented to comply with the Security Rule.

In Summary

The Organizational Requirements section of the Security Rule, among other things, provides requirements for the content of business associate contracts or other arrangements and the plan documents of group health plans. The Policies and Procedures and Documentation Requirements section, among other things, requires covered entities to implement and maintain written policies, procedures and documentation required to comply with the Security Rule.

Resources

The next paper in this series, paper #6 "Basics of Risk Analysis and Risk Management" outlines some of the general techniques used in risk analysis and risk management. Not all of the material discussed in the "Basics of Risk Analysis and Risk Management" paper will apply to all covered entities. The basic concepts and techniques discussed in this paper will be useful for most covered entities.

Covered entities should periodically check the CMS website at www.cms.hhs.gov under "Regulations and Guidance" for additional information and resources as they work through the security implementation process. There are many other sources of information available on the Internet. While CMS does not endorse guidance provided by other organizations, covered entities may also want to check with other local and national professional health care organizations, such as national provider and health plan associations for additional information.

Need more information?

Visit the CMS website often at www.cms.hhs.gov under "Regulations and Guidance" for the latest security papers, checklists, and announcements of upcoming events.

Visit the Office for Civil Rights website, http://www.hhs.gov/ocr/hipaa, for the latest guidance, FAQs 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)		
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)		
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)		
Workstation Security	§ 164.310(c)		
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)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)
ORGANIZATIONAL REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	**(R)**
		Availability	**(R)**
		Updates	**(R)**