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/SecurityStandard/ under the "Regulation" page.

HIPAA Administrative Simplification

- Privacy
- Electronic Transactions and Code Sets *
- National Identifiers
- Security

*** NOTE:** The original deadline for compliance with the transactions and code sets standards was October 16, 2002 for all covered entities except small health plans, which had until October 16, 2003 to comply.

The Administrative Simplification Compliance Act provided a one-year extension to covered entities that were not small health plans, if they timely submitted compliance plans to HHS.

NOTE: The definition of covered entities provided here summarizes the actual definitions found in the regulations. For the definitions of the three types of covered entities, see 45 C.F.R. § 160.103 which can be found at:

www.hhs.gov/ocr/hipaa

- **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).

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 & Other Arrangements
- Requirements for Group Health Plans

POLICIES & PROCEDURES & DOCUMENTATION REQUIREMENTS

- **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 www.cms.hhs.gov under "Regulations and Guidance". 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

NOTE: Addressable does not mean optional.

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

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

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.

- **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.

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

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 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. 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: 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, 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)**

2 Security Standards: Administrative Safeguards

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

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, commonly known as the Security Rule. 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 second paper in the series is devoted to the standards for Administrative Safeguards 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

An important step in protecting electronic protected health information (EPHI) is to implement reasonable and appropriate administrative safeguards that establish the foundation for a covered entity's security program. The Administrative Safeguards standards in the Security Rule, at § 164.308, were developed to accomplish this purpose.

The objectives of this paper are to:

- ❑ Review each Administrative Safeguards standard and implementation specification listed in the Security Rule.
- ❑ Discuss the purpose for each standard.
- ❑ Provide sample questions that covered entities may want to consider when implementing the Administrative Safeguards.

Sample questions provided in this paper, and other HIPAA Security Series papers, are for consideration only and are not required for implementation. The purpose of the sample questions is to promote review of a covered entity's environment in relation to the requirements of the Security Rule. The sample questions are not HHS interpretations of the requirements of the Security Rule.

All the information presented in the Security Series is designed to further covered entities' understanding of the Security Rule concepts. The papers are not intended to be the definitive guidance for covered entity compliance. Compliance with the Security Rule will depend on a number of factors, including those identified in § 164.306(b)(2):

"(i) The size, complexity, and capabilities of the covered entity.
(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
(iii) The costs of security measures.
(iv) The probability and criticality of potential risks to EPHI."

What are Administrative Safeguards?

The Security Rule defines administrative safeguards as, *"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."*

The Administrative Safeguards comprise over half of the HIPAA Security requirements. As with all the standards in this rule, compliance with the Administrative Safeguards standards will require an evaluation of the

security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of factors unique to each covered entity.

STANDARD § 164.308(a)(1) Security Management Process

The first standard under Administrative Safeguards section is the Security Management Process. This standard requires covered entities to:

> *"Implement policies and procedures to prevent, detect, contain and correct security violations."*

The purpose of this standard is to establish the administrative processes and procedures that a covered entity will use to implement the security program in its environment. There are four implementation specifications in the Security Management Process standard.

1. Risk Analysis (Required)
2. Risk Management (Required)
3. Sanction Policy (Required)
4. Information System Activity Review (Required)

NOTE: For a more detailed discussion of "addressable" and "required" implementation specifications, see the first paper in this series, "Security 101 for Covered Entities."

The Importance of Risk Analysis and Risk Management

Risk analysis and risk management are critical to a covered entity's Security Rule compliance efforts. Both are standard information security processes that have already been adopted by some organizations within the health care industry.

As stated in the responses to public comment in the preamble to the Security Rule, the Security Management Process standard and associated implementation specifications "*form the foundation upon which an entity's necessary security activities are built*." The results from the risk analysis and risk management processes will become the baseline for security processes within covered entities.

This paper provides a general understanding of risk analysis and risk management concepts and processes. CMS will include a more detailed discussion of risk analysis and risk management in paper 6 in the HIPAA Security Series titled, "Basics of Risk Analysis and Risk Management."

NOTE: Risk analysis and risk management serve as tools to assist in the development of a covered entity's strategy to protect the confidentiality, integrity, and availability of EPHI.

1. RISK ANALYSIS (R) - *§ 164.308(a)(1)(ii)(A)*

The Risk Analysis implementation specification requires covered entities to:

> *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*

In general, a risk analysis can be viewed as:

- ❑ The process of identifying potential security risks, and
- ❑ Determining the probability of occurrence and magnitude of risks.

Sample questions for covered entities to consider:

- ✓ How does EPHI flow throughout the organization? This includes EPHI that is created, received, maintained or transmitted by the covered entity.
- ✓ What are the less obvious sources of EPHI? Has the organization considered portable devices like PDAs?
- ✓ What are the external sources of EPHI? For example, do vendors or consultants create, receive, maintain or transmit EPHI?
- ✓ What are the human, natural, and environmental threats to information systems that contain EPHI?

2. RISK MANAGEMENT (R) - *§ 164.308(a)(1)(ii)(B)*

Risk Management is a required implementation specification. It requires an organization to make decisions about how to address security risks and vulnerabilities. The Risk Management implementation specification states that covered entities must:

> *"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."*

Risk management is the process used to identify and implement security measures to reduce risk to a reasonable and appropriate level within the covered entity based on the covered entity's circumstances. The measures implemented to comply with this required implementation specification must also allow the covered entity to comply with §

164.306(a) of the Security Standards: General Rules. Covered entities will want to answer some basic questions when planning their risk management process.

Sample questions for covered entities to consider:

- ✓ What security measures are already in place to protect EPHI (i.e., safeguards)?
- ✓ Is executive leadership and/or management involved in risk management and mitigation decisions?
- ✓ Are security processes being communicated throughout the organization?
- ✓ Does the covered entity need to engage other resources to assist in risk management?

In general, a covered entity will want to make sure its risk management strategy takes into account the characteristics of its environment including the factors at § 164.306(b)(2), which are listed on page 2 of this paper. These factors will help the covered entity to determine what potential security measures are reasonable and appropriate for its environment.

NOTE: Covered entities must ensure that the risk analysis and risk management processes are on-going and dynamic processes that can change as the environment or operations change.

3. SANCTION POLICY (R) - *§ 164.308(a)(1)(ii)(C)*

Another implementation specification in the Security Management Process is the Sanction Policy. It requires covered entities to:

> *"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."*

Appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with security policies and procedures, to deter noncompliance.

Sample questions for covered entities to consider:

- ✓ Does the covered entity have existing sanction policies and procedures to meet the requirements of this implementation specification? If not, can

existing sanction policies be modified to include language relating to violations of these policies and procedures?

✓ Does the organization require employees to sign a statement of adherence to security policy and procedures (e.g., as part of the employee handbook or confidentiality statement) as a prerequisite to employment?

✓ Does the statement of adherence to security policies and procedures state that the workforce member acknowledges that violations of security policies and procedures may lead to disciplinary action, for example, up to and including termination?

NOTE: A covered entity's sanction policy should reinforce its security policies and procedures.

✓ Does the sanction policy provide examples of potential violations of policy and procedures?

✓ Does the sanction policy adjust the disciplinary action based on the severity of the violation?

4. INFORMATION SYSTEM ACTIVITY REVIEW (R) - *§ 164.308(a)(1)(ii)(D)*

The Security Management Process standard also includes the Information System Activity Review implementation specification. This required implementation specification states that covered entities must:

> "*Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*"

The information system activity review enables covered entities to determine if any EPHI is used or disclosed in an inappropriate manner.

Information system activity review procedures may be different for each covered entity. The procedure should be customized to meet the covered entity's risk management strategy and take into account the capabilities of all information systems with EPHI.

Sample questions for covered entities to consider:

- ✓ What are the audit and activity review functions of the current information systems?
- ✓ Are the information systems functions adequately used and monitored to promote continual awareness of information system activity?
- ✓ What logs or reports are generated by the information systems?
- ✓ Is there a policy that establishes what reviews will be conducted?
- ✓ Is there a procedure that describes specifics of the reviews?

NOTE: The Information System Activity Review implementation specification should also promote continual awareness of any information system activity that could suggest a security incident.

STANDARD § 164.308(a)(2) Assigned Security Responsibility

The second standard in the Administrative Safeguards section is Assigned Security Responsibility. There are no separate implementation specifications for this standard. The standard requires that covered entities:

> *"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."*

The purpose of this standard is to identify who will be operationally responsible for assuring that the covered entity complies with the Security Rule. Covered entities should be aware of the following when assigning security responsibility:

- ❑ This requirement is comparable to the Privacy Rule standard at §164.530(a)(1), Personnel Designations, which requires all covered entities to designate a Privacy Official.
- ❑ The Security Official and Privacy Official can be the same person, but are not required to be.

- While one individual must be designated as having overall responsibility, other individuals in the covered entity may be assigned specific security responsibilities (e.g., facility security or network security).

When making this decision covered entities should consider some basic questions.

Sample questions for covered entities to consider:

- ✓ Would it serve the organization's needs to designate the same individual as both the Privacy and Security Official (for example, in a small provider office)?
- ✓ Has the organization agreed upon, and clearly identified and documented, the responsibilities of the Security Official?
- ✓ How are the roles and responsibilities of the Security Official crafted to reflect the size, complexity and technical capabilities of the organization?

STANDARD § 164.308(a)(3) Workforce Security

The third standard is Workforce Security, which states that covered entities must:

> *"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management standard*], *and to prevent those workforce members who do not have access under [the Information Access Management standard] from obtaining access to electronic protected health information."*

Within a covered entity's environment, workforce members that need access to EPHI to carry out their duties must be identified. For each workforce member, or job function, the covered entity must identify the EPHI that is needed, when it is needed, and make reasonable efforts to control access to the EPHI. This will also include identification of the computer systems and applications that provide access to the EPHI. Covered entities must provide only the minimum necessary access to EPHI that is required for a workforce member to do his or her job.

Within Workforce Security there are three addressable implementation specifications.

1. Authorization and/or Supervision (Addressable)

2. Workforce Clearance Procedure (Addressable)
3. Termination Procedures (Addressable)

1. AUTHORIZATION AND/OR SUPERVISION (A) – § *164.308(a)(3)(ii)(A)*

Where the Authorization and/or Supervision implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."*

Authorization is the process of determining whether a particular user (or a computer system) has the right to carry out a certain activity, such as reading a file or running a program. Implementation of this addressable implementation specification will vary among covered entities, depending upon the size and complexity of the workforce, and the information systems that contain EPHI. For example, in a very small provider office, all staff members may need to access all EPHI in their information system, since they may perform multiple functions. In this case, the covered entity might document the reasons for implementing policies and procedures allowing this kind of global access. If the documented rationale is reasonable and appropriate, this may be an acceptable approach.

NOTE: The Authorization and/or Supervision implementation specification provides the necessary checks and balances to ensure that all members of the workforce have appropriate access (or, in some cases, no access) to EPHI.

To determine the most reasonable and appropriate authorization and/or supervision procedures, covered entities may want to ask some basic questions about existing policies and procedures.

Sample questions for covered entities to consider:

- ✓ Are detailed job descriptions used to determine what level of access the person holding the position should have to EPHI?
- ✓ Who has or should have the authority to determine who can access EPHI, e.g., supervisors or managers?
- ✓ Are there similar existing processes used for paper records that could be used as an example for the EPHI?

Covered entities should review the authorization and supervision policies already present in the organization's current operating environment. Depending on the existing policies, covered entities may need to reinforce them, make modifications for EPHI, and/or develop corresponding documentation.

2. WORKFORCE CLEARANCE PROCEDURE (A) - *§ 164.308(a)(3)(ii)(B)*

Covered entities need to address whether all members of the workforce with authorized access to EPHI receive appropriate clearances. Where the Workforce Clearance Procedure implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."*

In other words, the clearance process must establish the procedures to verify that a workforce member does in fact have the appropriate access for their job function. A covered entity may choose to perform this type of screening procedure separate from or as a part of the authorization and/or supervision procedure.

Sample questions for covered entities to consider:

- ✓ Are there existing procedures for determining that the appropriate workforce members have access to the necessary information?
- ✓ Are the procedures used consistently within the organization when determining access of related workforce job functions?

3. TERMINATION PROCEDURES (A) - *§ 164.308(a)(3)(ii)(C)*

Where the Termination Procedures implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section."*

Termination procedures must be implemented to remove access privileges when an employee, contractor, or other individual previously entitled to access information no longer has these privileges. Whether the employee leaves the organization voluntarily or involuntarily, procedures to terminate access must be in place.

The same process that is implemented for termination should also be used to change access levels if an employee's job description changes to require more or less access to EPHI. The procedures should also address the complexity of the organization and the sophistication of associated information systems.

Sample questions for covered entities to consider:

- ✓ Do the termination policies and procedures assign responsibility for removing information system and/or physical access?
- ✓ Do the policies and procedures include timely communication of termination actions to insure that the termination procedures are appropriately followed?

STANDARD § 164.308(a)(4) Information Access Management

The fourth standard in the Administrative Safeguards section is Information Access Management. Covered entities are required to:

> *"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part [the Privacy Rule]."*

Restricting access to only those persons and entities with a need for access is a basic tenet of security. By implementing this standard, the risk of inappropriate disclosure, alteration, or destruction of EPHI is minimized. Covered entities must determine those persons and/or entities that need access to EPHI within their environment.

NOTE: The Information Access Management implementation specifications are closely related to the implementation specifications under the Workforce Security standard.

Compliance with this standard should support a covered entity's compliance with the HIPAA Privacy Rule minimum necessary requirements, which requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. To better understand this standard, covered entities should review the minimum necessary standard of the HIPAA Privacy Rule. See 45 CFR 164.502(b) and 164.514(d).

The Information Access Management standard has three implementation specifications.

1. Isolating Health Care Clearinghouse Functions (Required)

2. Access Authorization (Addressable)
3. Access Establishment and Modification (Addressable)

1. ISOLATING HEALTH CARE CLEARINGHOUSE FUNCTIONS (R) – *§ 164.308(a)(4)(ii)(A)*

The Isolating Health Care Clearinghouse Functions implementation specification states:

> *"If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization."*

This implementation specification only applies in the situation where a health care clearinghouse is part of a larger organization. In these situations, the health care clearinghouse is responsible for protecting the EPHI that it is processing.

Sample questions for covered entities to consider:

- ✓ Does the larger organization perform health care clearinghouse functions?
- ✓ If health care clearinghouse functions are performed, are policies and procedures implemented to protect EPHI from the other functions of the larger organization?
- ✓ Are additional technical safeguards needed to separate EPHI in information systems, used by the health care clearinghouse, to protect against unauthorized access by the larger organization?

2. ACCESS AUTHORIZATION (A) - § *164.308(a)(4)(ii)(B)*

In the Workforce Security standard portion of this paper, authorization was defined as the act of determining whether a particular user (or computer system) has the right, based on job function or responsibilities, to carry out a certain activity, such as reading a file or running a program. Where this implementation standard is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."*

Once the covered entity has determined that the person or system is authorized, there are numerous ways to grant access to EPHI. In general, a covered entity's policies and procedures must identify who has authority to grant access privileges. It must also state the process for granting access. To create and document policies and procedures to grant access, covered entities should address the following questions.

Sample questions for covered entities to consider:

- ✓ How is authorization documented? How can it be used to grant access?
- ✓ Are the policies and procedures for granting access consistent with applicable requirements of the Privacy Rule?
- ✓ Have appropriate authorization and clearance procedures, as specified in workforce security, been performed prior to granting access?
- ✓ Are access rules specific to applications and business requirements? For example, do different workforce members require different levels of access based on job function?
- ✓ Is there a technical process in place, such as creating unique user name and an authentication process, when granting access to a workforce member?

Once a covered entity has clearly defined who should get access to what EPHI and under what circumstances, it must consider how access is established and modified.

3. ACCESS ESTABLISHMENT AND MODIFICATION (A) - § *164.308(a)(4)(ii)(C)*

Where the Access Establishment and Modification implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."*

This means that a covered entity must implement and manage the creation and modification of access privileges to workstations, transactions, programs or processes. Responsibility for this function may be assigned to a specific individual or individuals, which also may be responsible for terminating access privileges for workforce members.

Covered entities must evaluate existing procedures, update them (if needed), and document procedures as necessary.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures in place for establishing access and modifying access?
- ✓ Are system access policies and procedures documented and updated as necessary?
- ✓ Do members of management or other workforce members periodically review the list of persons with access to EPHI to ensure they are valid and consistent with those authorized?

STANDARD § 164.308(a)(5) Security Awareness and Training

Regardless of the Administrative Safeguards a covered entity implements, those safeguards will not protect the EPHI if the workforce is unaware of its role in adhering to and enforcing them. Many security risks and vulnerabilities within covered entities are internal. This is why the next standard, Security Awareness and Training, is so important.

Specifically, the Security Awareness and Training standard states that covered entities must:

> *"Implement a security awareness and training program for all members of its workforce (including management)."*

Security training for all new and existing members of the covered entity's workforce is required by the compliance date of the Security Rule. In addition, periodic retraining should be given whenever environmental or operational changes affect the security of EPHI. Changes may include: new or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the Security Rule.

The Security Awareness and Training standard has four implementation specifications.

1. Security Reminders (Addressable)
2. Protection from Malicious Software (Addressable)
3. Log-in Monitoring (Addressable)
4. Password Management (Addressable)

1. SECURITY REMINDERS (A) - *§ 164.308(a)(5)(ii)(A)*

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

> *"Periodic security updates."*

There are many types of security reminders that covered entities may choose to implement. Examples might include notices in printed or electronic form, agenda items and specific discussion topics at monthly meetings, focused reminders posted in affected areas, as well as formal retraining on security policies and procedures. Covered entities should look at how they currently remind the workforce of current policies and procedures, and then decide whether these practices are reasonable and appropriate or if other forms of security reminders are needed.

NOTE: Covered entities must document the security reminders they implement. Documentation could include the type of reminder, its message, and the date it was implemented.

2. PROTECTION FROM MALICIOUS SOFTWARE (A) - § *164.308(a)(5)(ii)(B)*

One important security measure that employees may need to be reminded of is security software that is used to protect against malicious software. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

> *"Procedures for guarding against, detecting, and reporting malicious software."*

Malicious software can be thought of as any program that harms information systems, such as viruses, Trojan horses or worms. As a result of an unauthorized infiltration, EPHI and other data can be damaged or destroyed, or at a minimum, require expensive and time-consuming repairs.

NOTE: Malicious software that successfully invades information systems can cause significant damage.

Malicious software is frequently brought into an organization through email attachments, and programs that are downloaded from the Internet. Under the Security Awareness and Training standard, the workforce must also be trained regarding its role in protecting against malicious software, and system protection capabilities. It is important to note that training must be an ongoing process for all organizations.

3. LOG-IN MONITORING (A) - § *164.308(a)(5)(ii)(C)*

Security awareness and training should also address how users log onto systems and how they are supposed to manage their passwords. Where the Log-in Monitoring implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

"Procedures for monitoring log-in attempts and reporting discrepancies."

Typically, an inappropriate or attempted log-in is when someone enters multiple combinations of usernames and/or passwords to attempt to access an information system. Fortunately, many information systems can be set to identify multiple unsuccessful attempts to log-in. Other systems might record the attempts in a log or audit trail. Still others might require resetting of a password after a specified number of unsuccessful log-in attempts.

NOTE: The purpose of the Log-in Monitoring implementation specification is to make workforce members aware of log-in attempts that are not appropriate.

If smaller covered entities are not using, or are not familiar with, their systems capabilities for these types of log-in attempts, they should contact their system vendor or read their application software manuals for more information. Once capabilities are established the workforce must be made aware of how to use and monitor them.

4. PASSWORD MANAGEMENT - § *164.308(a)(5)(ii)(D)*

The last addressable specification in this standard is Password Management. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

"Procedures for creating, changing, and safeguarding passwords."

In addition to providing a password for access, entities must ensure that workforce members are trained on how to safeguard the information. Covered entities must train all users and establish guidelines for creating passwords and changing them during periodic change cycles.

Sample questions for covered entities to consider:

- ✓ Are there policies in place that prevent workforce members from sharing passwords with others?
- ✓ Is the workforce advised to commit their passwords to memory?

- ✓ Are common sense precautions taken, such as not writing passwords down and leaving them in areas that are visible or accessible to others?

STANDARD § 164.308(a)(6) Security Incident Procedures

The next standard is Security Incident Procedures, which states that covered entities must:

"Implement policies and procedures to address security incidents."

The purpose of this standard is to require covered entities to address security incidents within their environment. Addressing security incidents is an integral part of the overall security program. Implementing the Security Rule standards will reduce the type and amount of security incidents a covered entity encounters, but security incidents will occur. Even covered entities with detailed security policies and procedures and advanced technology will have security incidents.

The Security Rule defines a security incident as, *"the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."* Security incident procedures must address how to identify security incidents and provide that the incident be reported to the appropriate person or persons.

Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other Security Rule standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

There is one required implementation specification for this standard.

RESPONSE AND REPORTING (R) - § *164.308(a)(6)(ii)*

The Response and Reporting implementation specification states that covered entities must:

> *"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."*

Security incident procedures must describe how workforce members are to respond to an incident. This may include: preserving evidence; mitigating, to the extent possible, the situation that caused the incident; documenting the incident and the outcome; and evaluating security incidents as part of ongoing risk management.

Covered entities must be aware of any number of possible incidents that they may have to deal with. For example:

- Stolen or otherwise inappropriately obtained passwords that are used to access EPHI
- Corrupted backup tapes that do not allow restoration of EPHI
- Virus attacks that interfere with the operations of information systems with EPHI
- Physical break-ins leading to the theft of media with EPHI
- Failure to terminate the account of a former employee that is then used by an unauthorized user to access information systems with EPHI
- Providing media with EPHI, such as a PC hard drive or laptop, to another user who is not authorized to access the EPHI prior to removing the EPHI stored on the media.

A covered entity's security incident procedures must establish adequate response and reporting procedures for these and other types of events.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented to address security incidents?
- ✓ Do the security incident policies and procedures list possible types of security incidents and the response for each?
- ✓ Do the security incident policies and procedures identify to whom security incidents must be reported?

STANDARD § 164.308(a)(7) Contingency Plan

The purpose of contingency planning is to establish strategies for recovering access to EPHI should the organization experience an emergency or other occurrence, such as a power outage and/or disruption of critical business operations. The goal is to ensure that organizations have their EPHI available when it is needed. The Contingency Plan standard requires that covered entities:

> *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*

The Contingency Plan standard includes five implementation specifications.

1. Data Backup Plan (Required)
2. Disaster Recovery Plan (Required)
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

1. DATA BACKUP PLAN (R) - § *164.308(a)(7)(ii)(A)*

The Data Backup Plan implementation specification requires covered entities to:

> *"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."*

Most covered entities may have backup procedures as part of current business practices. Data Backup plans are an important safeguard for all covered entities, and a required implementation specification.

Sample questions for covered entities to consider:

- ✓ What is the EPHI that must be backed up?
- ✓ Does the plan include all important sources of data such as patient accounting systems, electronic medical records, health maintenance and case management information, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used?

- ✓ Has the organization considered the various methods of backups, including tape, disk, or CD?
- ✓ Does the backup plan include storage of backups in a safe, secure place?
- ✓ Is the organization's frequency of backups appropriate for its environment?

2. DISASTER RECOVERY PLAN (R) - § *164.308(a)(7)(ii)(B)*

The Disaster Recovery Plan implementation specification requires covered entities to:

> *"Establish (and implement as needed) procedures to restore any loss of data."*

Some covered entities may already have a general disaster plan that meets this requirement; however, each entity must review the current plan to ensure that it allows them to recover EPHI.

Sample questions for covered entities to consider:

- ✓ Does the disaster recovery plan address issues specific to the covered entity's operating environment?
- ✓ Does the plan address what data is to be restored?
- ✓ Is a copy of the disaster recovery plan readily accessible at more than one location?

3. EMERGENCY MODE OPERATION PLAN (R) - § *164.308(a)(7)(ii)(C)*

The Emergency Mode Operation Plan implementation specification requires covered entities to:

> *"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."*

When a covered entity is operating in emergency mode due to a technical failure or power outage, security processes to protect EPHI must be maintained.

Sample questions for covered entities to consider:

- ✓ Does the organization's plan balance the need to protect the data with the organization's need to access the data?
- ✓ Will alternative security measures be used to protect the EPHI?
- ✓ Does the emergency mode operation plan include possible manual procedures for security protection that can be implemented as needed?
- ✓ Does the emergency mode operation plan include telephone numbers and contact names for all persons that must be notified in the event of a disaster, as well as roles and responsibilities of those people involved in the restoration process?

4. TESTING AND REVISION PROCEDURES (A) - § *164.308(a)(7)(ii)(D)*

Where the Testing and Revision Procedures implementation specification is a reasonable and appropriate safeguard for the covered entity, the covered entity must:

> *"Implement procedures for periodic testing and revision of contingency plans."*

It is important to point out that this implementation specification applies to all implementation specifications under the Contingency Plan standard, including the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.

NOTE: Testing and revision procedures will vary in frequency and comprehensiveness.

Disaster recovery and emergency mode operations plans might be tested by using a scenario-based walk-thru (to avoid daily operations impacts) or by performing complete live tests. The comprehensiveness and sophistication of the testing and revision procedures depends on the complexity of the covered entity's organization and other factors such as size and costs. It is expected that the frequency and comprehensiveness of the procedures will vary among covered entities.

Sample questions for covered entities to consider:

- ✓ Are the processes for restoring data from backups, disaster recovery and emergency mode operation documented?

- ✓ Do those responsible for performing contingency planning tasks understand their responsibilities?
- ✓ Have those responsible actually performed a test of the procedures?
- ✓ Have the results of each test been documented and any problems with the test reviewed and corrected?

NOTE: In most environments, at a minimum, a covered entity should determine if existing contingency plans are appropriate.

5. APPLICATION AND DATA CRITICALITY ANALYSIS (A) - § *164.308(a)(7)(ii)(E)*

The last implementation specification in the Contingency Plan standard is Application and Data Criticality Analysis. Where this implementation specification is a reasonable and appropriate safeguard for the covered entity, the covered entity must:

> *"Assess the relative criticality of specific applications and data in support of other contingency plan components."*

This implementation specification requires covered entities to identify their software applications (data applications that store, maintain or transmit EPHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operations plans. A prioritized list of specific applications and data will help determine which applications or information systems get restored first and/or which must be available at all times.

STANDARD § 164.308(a)(8) Evaluation

It is important for a covered entity to know if the security plans and procedures it implements continue to adequately protect its EPHI. To accomplish this, covered entities must implement ongoing monitoring and evaluation plans. Covered entities must periodically evaluate their strategy and systems to ensure that the security requirements continue to meet their organizations' operating environments.

The Evaluation standard has no separate implementation specifications. The standard requires covered entities to:

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule]."

NOTE: On-going evaluation of security measures is the best way to ensure all EPHI is adequately protected.

The purpose of the evaluation is to establish a process for covered entities to review and maintain reasonable and appropriate security measures to comply with the Security Rule. Initially the evaluation must be based on the security standards implemented to comply with the Security Rule. Subsequent periodic evaluations must be performed in response to environmental or operational changes that affect the security of EPHI. The on-going evaluation should also be performed on a scheduled basis, such as annually or every two years. The evaluation must include reviews of the technical and non-technical aspects of the security program.

Sample questions for covered entities to consider:

- ✓ How often should an evaluation be done? For example, are additional evaluations performed if security incidents are identified, changes are made in the organization, or new technology is implemented?
- ✓ Is an internal or external evaluation, or a combination of both, most appropriate for the covered entity?
- ✓ Are periodic evaluation reports and the supporting material considered in the analysis, recommendations, and subsequent changes fully documented?

STANDARD § 164.308(b)(1) Business Associate Contracts And Other Arrangements

The last standard in the Administrative Safeguards section is Business Associate Contracts and Other Arrangements. The organizational requirements related to this standard are discussed in more detail in § 164.314(a) of the Rule, which is covered in paper five of this series titled "Security Standards – Organizational, Policies and Procedures and Documentation Requirements." The Business Associate Contracts and Other Arrangements standard states that:

"A covered entity, in accordance with § 164.306 [the Security Standards: General Rules], may permit a business associate to create, receive,

maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) [the Organizational Requirements] that the business associate will appropriately safeguard the information (Emphasis added)."

Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. This standard is comparable to the Business Associate Contract standard in the Privacy Rule, but is specific to business associates that create, receive, maintain or transmit EPHI. To comply with this standard, covered entities must obtain satisfactory assurances from the business associate that it will appropriately safeguard EPHI.

This standard also addresses a few situations in which a business associate contract is not needed.

As stated at § 164.308(b)(2), the Business Associate Contracts and Other Arrangements standard does not apply with respect to:

"(i) The transmission by a covered entity of EPHI to a health care provider concerning the treatment of an individual.

(ii) The transmission of EPHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of EPHI from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met."

In addition, § 164.308(b)(3) states, *"A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a)."*

The standard has one implementation specification.

WRITTEN CONTRACT OR OTHER ARRANGEMENT (R) – *§ 164.308(b)(4)*

Covered entities are required to:

"Document the satisfactory assurances required by paragraph (b)(1) [the Business Associate Contracts and Other Arrangements] of this section

through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [the Organizational Requirements].”

Sample questions covered entities may want to consider:

- ✓ Have all business associates been identified? Business associates may include clearinghouses, medical billing services, vendors of hardware and software, external consultants, lawyers, transcription contractors, or others who have access to EPHI.

- ✓ Have existing business associate contracts created and implemented for compliance with the Privacy Rule, which involve EPHI, been reviewed to determine if Security Rule requirements are addressed?

- ✓ To minimize additional work efforts, can existing business associate contracts, which involve EPHI, be modified to include Security Rule requirements?

In Summary

All of the standards and implementation specifications found in the Administrative Safeguards section refer to administrative functions, such as policy and procedures that must be in place for management and execution of security measures. These include performance of security management process, assignment or delegation of security responsibility, training requirements, and evaluation and documentation of all decisions.

Resources

The remaining papers in this series will address other specific topics related to the Security Rule. The next paper in this series covers the Physical Safeguards section. These are the safeguards required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion, as well as the measures necessary to restrict physical access to EPHI.

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)**

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

3 Security Standards: Physical Safeguards

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. This series aims to explain 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 third paper in the series is devoted to the standards for Physical Safeguards 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

An important step in protecting electronic protected health information (EPHI) is to implement reasonable and appropriate physical safeguards for information systems and related equipment and facilities. The Physical Safeguards standards in the Security Rule were developed to accomplish this purpose. As with all the standards in this rule, compliance with the Physical Safeguards standards will require an

evaluation of the security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of factors unique to each covered entity.

The objectives of this paper are to:

- Review each Physical Safeguard standard and implementation specification listed in the Security Rule.
- Discuss physical vulnerabilities and provide examples of physical controls that may be implemented in a covered entity's environment.
- Provide sample questions that covered entities may want to consider when implementing the Physical Safeguards.

What are physical safeguards?

The Security Rule defines physical safeguards as *"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."* The standards are another line of defense (adding to the Security Rule's administrative and technical safeguards) for protecting EPHI.

When evaluating and implementing these standards, a covered entity must consider all physical access to EPHI. This may extend outside of an actual office, and could include workforce members' homes or other physical locations where they access EPHI.

NOTE: A matrix of all of the Security Rule Standards and Implementation Specifications is included at the end of this paper.

STANDARD § 164.310(a)(1) Facility Access Controls

The first standard under the Physical Safeguards section is Facility Access Control. It requires covered entities to:

"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

A facility is defined in the rule as *"the physical premises and the interior and exterior of a building(s)"*.

NOTE: For a more detailed discussion of "addressable" and "required" implementation specifications, see the first paper in this series, "Security 101 for Covered Entities."

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facility or facilities in which they are housed?
- ✓ Do the policies and procedures identify individuals (workforce members, business associates, contractors, etc.) with authorized access by title and/or job function?
- ✓ Do the policies and procedures specify the methods used to control physical access such as door locks, electronic access control systems, security officers, or video monitoring?

The Facility Access Controls standard has four implementation specifications.

1. Contingency Operations (Addressable)
2. Facility Security Plan (Addressable)
3. Access Control and Validation Procedures (Addressable)
4. Maintenance Records (Addressable)

1. CONTINGENCY OPERATIONS (A) - *§ 164.310(a)(2)(i)*

The Contingency Operations implementation specification refers to physical security measures entities establish in the event of the activation of contingency plans and employ while the contingency plans required by the Administrative Safeguards are active.

NOTE: Facility access controls implementation specifications are addressable. This means that access controls during contingency operations may vary significantly from entity to entity.

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency."*

Contingency operations may be set in motion during or immediately following a disaster or emergency situation. During contingency operations, it is important to

maintain physical security and appropriate access to EPHI while allowing for data restoration activities.

Facility access controls during contingency operations will vary significantly from entity to entity. For example, a large covered entity may need to post guards at entrances to the facility or have escorts for individuals authorized to access the facility for data restoration purposes. For smaller operations, it may be sufficient to have all staff involved in the recovery process.

Sample questions for covered entities to consider:

- ✓ Are procedures developed to allow facility access while restoring lost data in the event of an emergency, such as a loss of power?
- ✓ Can the procedures be appropriately implemented, as needed, by those workforce members responsible for the data restoration process?
- ✓ Do the procedures identify personnel that are allowed to re-enter the facility to perform data restoration?
- ✓ Is the content of this procedure also addressed in the entity's contingency plan? If so, should the content be combined?

2. FACILITY SECURITY PLAN (A) - *§ 164.310(a)(2)(ii)*

The Facility Security Plan defines and documents the safeguards used by the covered entity to protect the facility or facilities.

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."*

NOTE: Facility security plans document the use of physical access controls.

Facility security plans must document the use of physical access controls. These controls must ensure that only authorized individuals have access to facilities and equipment that contain EPHI. In general, physical access controls allow individuals with legitimate business needs to obtain access to the facility and deny access to those without legitimate business needs. Procedures must also be used to prevent tampering and theft of EPHI and related equipment.

To establish the facility security plan, covered entities should review risk analysis data on persons or workforce members that need access to facilities and equipment. This includes staff, patients, visitors and business partners.

Some common controls to prevent unauthorized physical access, tampering, and theft that covered entities may want to consider include:

- Locked doors, signs warning of restricted areas, surveillance cameras, alarms
- Property controls such as property control tags, engraving on equipment
- Personnel controls such as identification badges, visitor badges and/or escorts for large offices
- Private security service or patrol for the facility

In addition, all staff or employees must know their roles in facility security. Covered entities must review the plan periodically, especially when there are any significant changes in the environment or information systems.

NOTE: The facility security plan should be an integral part of a covered entity's daily operations.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented to protect the facility and associated equipment against unauthorized physical access, tampering, and theft?
- ✓ Do the policies and procedures identify controls to prevent unauthorized physical access, tampering, and theft, such as those listed in the common controls to consider bullets above?

3. ACCESS CONTROL AND VALIDATION PROCEDURES (A) - *§ 164.310(a)(2)(iii)*

The Facility Access Controls standard also includes the Access Control and Validation Procedures implementation specification. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."*

The purpose of this implementation specification is to specifically align a person's access to information with his or her role or function in the organization. These functional or role-based access control and validation procedures should be closely aligned with the facility security plan. These procedures are the means by which a covered entity will actually determine the workforce members or persons that should have access to certain locations within the facility based on their role or function.

NOTE: The Security Rule requires that a covered entity document the rationale for all security decisions.

The controls implemented will depend on the covered entity's environmental characteristics. For example, it is common practice to question a person's identity by asking for proof of identity, such as a picture ID, before allowing access to a facility. In a large organization, because of the number of visitors and employees, this practice may be required for every visit. In a small doctor's office, once someone's identity has been verified it may not be necessary to check identity every time he or she visits, because the identity would already be known.

Sample questions for covered entities to consider:

- ✓ Are procedures developed and implemented to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision?
- ✓ Do the procedures identify the methods for controlling and validating an employee's access to facilities, such as the use of guards, identification badges, or entry devices such as key cards?
- ✓ Do the procedures also identify visitor controls, such as requiring them to sign in, wear visitor badges and be escorted by an authorized person?
- ✓ Do the procedures identify individuals, roles or job functions that are authorized to access software programs for the purpose of testing and revision in order to reduce errors?
- ✓ Does management regularly review the lists of individuals with physical access to sensitive facilities?

4. MAINTENANCE RECORDS (A) - *§ 164.310(a)(2)(iv)*

Covered entities may make many types of facility security repairs and modifications on a regular basis, including changing locks, making routine maintenance checks and installing new security devices.

The Maintenance Records implementation specification requires that covered entities document such repairs and changes. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks)."*

In a small office, documentation may simply be a logbook that notes the date, reason for repair or modification and who authorized it. In a large organization, various repairs and modifications of physical security components may need to be documented in more detail and maintained in a database.

NOTE: Documentation of maintenance records may vary from a simple logbook to a comprehensive database.

In some covered entities the most frequent physical security changes may be re-keying door locks or changing the combination on a door, when someone from the workforce has been terminated. Some facilities may use door locks that rely on a card or badge reader. Documentation on the repair, addition, or removal of these devices may also be needed to meet this specification.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented that specify how to document repairs and modifications to the physical components of a facility which are related to security?
- ✓ Do the policies and procedures specify all physical security components that require documentation?
- ✓ Do the policies and procedures specify special circumstances when repairs or modifications to physical security components are required, such as, when certain workforce members (e.g., Application Administrators) with access to large amounts of EPHI are terminated?

STANDARD § 164.310(b) Workstation Use

The next standard in the Physical Safeguards is Workstation Use. A workstation is defined in the rule as *"an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."*

The Workstation Use standard requires covered entities to specify the proper functions to be performed by electronic computing devices. Inappropriate use of computer workstations can expose a covered entity to risks, such as virus attacks, compromise of information systems, and breaches of confidentiality. This standard has no implementation specifications, but like all standards must be implemented. The proper environment for workstations is another topic that this standard covers.

NOTE: The Workstation Use and Workstation Security standards have no implementation specifications, but like all standards must be implemented.

For this standard, covered entities must:

> *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."*

Many covered entities may have existing policies and procedures that address appropriate business use of workstations. In these cases, it may be possible for them to update existing documentation to address security issues. Covered entities must assess their physical surroundings to ensure that any risks associated with a workstation's surroundings are known and analyzed for a possible negative impact.

The Workstation Use standard also applies to covered entities with workforce members that work off site using workstations that can access EPHI. This includes employees who work from home, in satellite offices, or in another facility. Workstation policies and procedures must specify the proper functions to be performed, regardless of where the workstation is located.

NOTE: At a minimum, all safeguards required for office workstations must also be applied to workstations located off site.

Some common practices that may already be in place include logging off before leaving a workstation for an extended period of time, and using and continually updating antivirus software.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI?
- ✓ Do the policies and procedures identify workstations that access EPHI and those that do not?

- ✓ Do the policies and procedures specify where to place and position workstations to only allow viewing by authorized individuals?
- ✓ Do the policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as using privacy screens, enabling password protected screen savers or logging off the workstation?
- ✓ Do the policies and procedures address workstation use for users that access EPHI from remote locations (i.e., satellite offices or telecommuters)?

STANDARD § 164.310(c) Workstation Security

Like Workstation Use, Workstation Security is a standard with no implementation specifications. The Workstation Security standard requires that covered entities:

> *"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."*

While the Workstation Use standard addresses the policies and procedures for how workstations should be used and protected, the Workstation Security standard addresses how workstations are to be physically protected from unauthorized users.

Covered entities may implement a variety of strategies to restrict access to workstations with EPHI. One way may be to completely restrict physical access to the workstation by keeping it in a secure room where only authorized personnel work.

As with all standards and implementation specifications, what is reasonable and appropriate for one covered entity may not apply to another. The risk analysis should be used to help with the decision-making process.

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

Sample questions for covered entities to consider:

- ✓ Are physical safeguards implemented for all workstations that access EPHI, to restrict access to authorized users?
- ✓ Have all types of workstations that access EPHI been identified, such as laptops, desktop computers, personal digital assistants (PDAs)?
- ✓ Are current physical safeguards used to protect workstations with EPHI effective?
- ✓ Are additional physical safeguards needed to protect workstations with EPHI?

- ✓ Are the physical safeguards used to protect workstations that access EPHI documented in the Workstation Use policies and procedures?

STANDARD § 164.310(d)(1) Device and Media Controls

The Device and Media Controls standard requires covered entities to:

> *"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility."*

As referenced here, the term "electronic media" means, *"electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card…"* This standard covers the proper handling of electronic media including receipt, removal, backup, storage, reuse, disposal and accountability.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented that govern the receipt and removal of hardware and electronic media that contain EPHI, into and out of a facility, and the movement of these items within the facility?
- ✓ Do the policies and procedures identify the types of hardware and electronic media that must be tracked?
- ✓ Have all types of hardware and electronic media that must be tracked been identified, such as, hard drives, magnetic tapes or disks, optical disks or digital memory cards?

The Device and Media Controls standard has four implementation specifications, two required and two addressable.

1. Disposal (Required)
2. Media Re-Use (Required)
3. Accountability (Addressable)
4. Data Backup and Storage (Addressable)

1. DISPOSAL (R) - *§ 164.310(d)(2)(i)*

The Disposal implementation specification states that covered entities must:

> *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."*

When covered entities dispose of any electronic media that contains EPHI they should make sure it is unusable and/or inaccessible. One way to dispose of electronic media is by degaussing. Degaussing is a method whereby a strong magnetic field is applied to magnetic media to fully erase the data. If a covered entity does not have access to degaussing equipment, another way to dispose of the electronic media is to physically damage it beyond repair, making the data inaccessible.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented that address disposal of EPHI, and/or the hardware or electronic media on which it is stored?
- ✓ Do the policies and procedures specify the process for making EPHI, and/or the hardware or electronic media, unusable and inaccessible?
- ✓ Do the policies and procedures specify the use of a technology, such as, software or a specialized piece of hardware, to make EPHI, and/or the hardware or electronic media, unusable and inaccessible?
- ✓ Are the procedures used by personnel authorized to dispose of EPHI, and/or the hardware or electronic media?

2. MEDIA RE-USE (R) - *§ 164.310(d)(2)(ii)*

Instead of disposing of electronic media, covered entities may want to reuse it. Media Re-Use, a required implementation specification for this standard, states that covered entities must:

> *"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."*

In addition to appropriate disposal, covered entities must appropriately reuse electronic media, whether for internal or external use. Internal re-use may include re-deployment of PCs or sharing floppy disks. External re-use may include donation of electronic media to charity organizations or local schools. In either of these instances, it is important to remove all EPHI previously stored on the media to prevent unauthorized access to the information.

Covered entities should consider the following when developing a re-use procedure.

Sample questions for covered entities to consider:

- ✓ Are procedures developed and implemented for removal of EPHI from electronic media before re-use?

- ✓ Do the procedures specify situations when all EPHI must be permanently deleted or situations when the electronic media should only be reformatted so that no files are accessible?

The following two implementation specifications for this standard, Accountability and Data Backup and Storage, are addressable.

3. ACCOUNTABILITY (A) - *§ 164.310(d)(2)(iii)*

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."*

Since this is an addressable specification, each covered entity must determine if and how it should be implemented for their organization. If a covered entity's hardware and media containing EPHI are moved from one location to another, a record should be maintained as documentation of the move.

Portable workstations and media present a special accountability challenge. Portable technology is getting smaller, less expensive, and has an increased capacity to store large quantities of data. As a result, it is becoming more prevalent in the health care industry, making accountability even more important and challenging.

Some questions covered entities may want to address when implementing the accountability specification include the following.

Sample questions for covered entities to consider:

- ✓ Is a process implemented for maintaining a record of the movements of, and person(s) responsible for, hardware and electronic media containing EPHI?

- ✓ Have all types of hardware and electronic media that must be tracked been identified, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards?

- ✓ If there are multiple devices of the same type, is there a way to identify individual devices and log or record them separately, such as a serial numbers or other tracking mechanisms?

4. DATA BACKUP AND STORAGE (A) - *§ 164.310(d)(2)(iv)*

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."*

This specification protects the availability of EPHI and is similar to the Data Backup Plan implementation specification for the contingency plan standard of the Administrative Safeguards, which requires covered entities to implement procedures to create and maintain retrievable exact copies of EPHI. Therefore, both implementation specifications may be included in the same policies and procedures. A covered entity may choose to backup a hard drive before moving to prevent loss of EPHI when the existing data backup plan does not provide for local hard drive backups. Another option may be to limit where computer users store their files. For example, larger organizations may implement policies that require users to save all information on the network, thus eliminating the need for a hard drive back up prior to the move. Either of these options, and others, may be considered reasonable and appropriate solutions, depending on the covered entity's environment.

Sample questions for covered entities to consider:

- ✓ Is a process implemented for creating a retrievable, exact copy of EPHI, when needed, before movement of equipment?
- ✓ Does the process identify situations when creating a retrievable, exact copy of EPHI is required and situations when not required before movement of equipment?
- ✓ Does the process identify who is responsible for creating a retrievable, exact copy of EPHI before movement of equipment?

In Summary

The Security Rule's Physical Safeguards are the physical measures, policies and procedures to protect electronic information systems, buildings and equipment. Successfully implemented, these standards and implementation specifications should help protect covered entities' EPHI from natural and environmental hazards, as well as unauthorized intrusion. All of the Physical Safeguards are designed to protect the confidentiality, integrity, and accessibility of EPHI.

Resources

The remaining papers in this series will address other specific topics related to the Security Rule. The next paper in this series covers the Security Rule's Technical Safeguards. The Technical Safeguards are the technology, policies and related corresponding procedures that protect EPHI and control access to it.

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.

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

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 Procedures	(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 Procedure	(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)**

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**

4 Security Standards: Technical Safeguards

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, commonly known as the Security Rule. 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 had until April 20, 2006 to comply.

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 fourth paper in the series is devoted to the standards for Technical Safeguards 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/*** under the "Regulation & Guidance" page.

Background

Technical safeguards are becoming increasingly more important due to technology advancements in the health care industry. As technology improves, new security challenges emerge. Healthcare organizations are faced with the challenge of protecting electronic protected health information (EPHI), such as electronic health records, from various internal and external risks. To reduce risks to EPHI, covered entities must implement technical safeguards. Implementation of the Technical Safeguards standards

represent good business practices for technology and associated technical policies and procedures within a covered entity. It is important, and therefore required by the Security Rule, for a covered entity to comply with the Technical Safeguard standards and certain implementation specifications; a covered entity may use any security measures that allow it to reasonably and appropriately do so.

The objectives of this paper are to:

- Review each Technical Safeguards standard and implementation specification listed in the Security Rule.
- Discuss the purpose for each standard.
- Provide sample questions that covered entities may want to consider when implementing the Technical Safeguards.

Sample questions provided in this paper, and other HIPAA Security Series papers, are for consideration only and are not required for implementation. The purpose of the sample questions is to promote review of a covered entity's environment in relation to the requirements of the Security Rule. The sample questions are not HHS interpretations of the requirements of the Security Rule.

What are Technical Safeguards?

The Security Rule defines technical safeguards in § 164.304 as *"the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."*

As outlined in previous papers in this series, the Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The Rule allows a covered entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications. A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.

45 CFR § 164.306(b), the Security Standards: General Rules, Flexibility of Approach, provides key guidance for focusing compliance decisions, including factors a covered entity must consider when selecting security

measures such as technology solutions. In addition, the results of the required risk analysis and risk management processes at §§ 164.308(a)(1)(ii)(A) & (B) will also assist the entity to make informed decisions regarding which security measures to implement.

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

The Security Rule does not require specific technology solutions. In this paper, some security measures and technical solutions are provided as examples to illustrate the standards and implementation specifications. These are only examples. There are many technical security tools, products, and solutions that a covered entity may select. Determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for their specific organization, given their own unique characteristics, as specified in § 164.306(b) the Security Standards: General Rules, Flexibility of Approach.

Some solutions may be costly, especially for smaller covered entities. While cost is one factor a covered entity may consider when deciding on the implementation of a particular security measure, it is not the only factor. The Security Rule is clear that reasonable and appropriate security measures must be implemented, see 45 CFR 164.306(b), and that the General Requirements of § 164.306(a) must be met.

NOTE: A covered entity must establish a balance between the identifiable risks and vulnerabilities to EPHI, the cost of various protective measures and the size, complexity, and capabilities of the entity, as provided in § 164.306(b)(2).

STANDARD § 164.312(a)(1) Access Control

The Security Rule defines access in § 164.304 as *"the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part [the HIPAA Privacy Rule])."* Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules that the covered entity is required to implement as part of § 164.308(a)(4), the Information Access Management standard under the Administrative Safeguards section of the Rule.

NOTE: For more information on Information Access Management, see paper 2 in this series, "Security Standards – Administrative Safeguards."

The Access Control standard requires a covered entity to:

> *"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)[Information Access Management]."*

A covered entity can comply with this standard through a combination of access control methods and technical controls. There are a variety of access control methods and technical controls that are available within most information systems. The Security Rule does not identify a specific type of access control method or technology to implement.

Regardless of the technology or information system used, access controls should be appropriate for the role and/or function of the workforce member. For example, even workforce members responsible for monitoring and administering information systems with EPHI, such as administrators or super users, must only have access to EPHI as appropriate for their role and/or job function.

NOTE: For a discussion on "required" and "addressable" Implementation Specifications, see the first paper in this series, "Security 101 for Covered Entities."

Four implementation specifications are associated with the Access Controls standard.

1. Unique User Identification (Required)
2. Emergency Access Procedure (Required)
3. Automatic Logoff (Addressable)
4. Encryption and Decryption (Addressable)

1. UNIQUE USER IDENTIFICATION (R) - § 164.312(a)(2)(i)

The Unique User Identification implementation specification states that a covered entity must:

> *"Assign a unique name and/or number for identifying and tracking user identity."*

User identification is a way to identify a specific user of an information system, typically by name and/or number. A unique user identifier allows an entity to track specific user activity when that user is logged into an information system. It enables an entity to hold users accountable for functions performed on information systems with EPHI when logged into those systems.

The Rule does not describe or provide a single format for user identification. Covered entities must determine the best user identification strategy based on their workforce and

operations. Some organizations may use the employee name or a variation of the name (e.g. jsmith). However, other organizations may choose an alternative such as assignment of a set of random numbers and characters. A randomly assigned user identifier is more difficult for an unauthorized user (e.g., a hacker) to guess, but may also be more difficult for authorized users to remember and management to recognize. The organization must weigh these factors when making its decision. Regardless of the format, unlike email addresses, no one other than the user needs to remember the user identifier.

Sample questions for covered entities to consider:

- ✓ Does each workforce member have a unique user identifier?
- ✓ What is the current format used for unique user identification?
- ✓ Can the unique user identifier be used to track user activity within information systems that contain EPHI?

2. EMERGENCY ACCESS PROCEDURE (R) - § 164.312(a)(2)(ii)

This implementation specification requires a covered entity to:

> *"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."*

These procedures are documented instructions and operational practices for obtaining access to necessary EPHI during an emergency situation. Access controls are necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. Covered entities must determine the types of situations that would require emergency access to an information system or application that contains EPHI.

NOTE: Like many of the Technical Safeguards implementation specifications, covered entities may already have emergency access procedures in place.

Procedures must be established beforehand to instruct workforce members on possible ways to gain access to needed EPHI in, for example, a situation in which normal environmental systems, such as electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster.

Sample questions for covered entities to consider:

- ✓ Who needs access to the EPHI in the event of an emergency?
- ✓ Are there policies and procedures in place to provide appropriate access to EPHI in emergency situations?

3. AUTOMATIC LOGOFF (A) - § 164.312(a)(2)(iii)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*

As a general practice, users should logoff the system they are working on when their workstation is unattended. However, there will be times when workers may not have the time, or will not remember, to log off a workstation. Automatic logoff is an effective way to prevent unauthorized users from accessing EPHI on a workstation when it is left unattended for a period of time.

Many applications have configuration settings for automatic logoff. After a predetermined period of inactivity the application will automatically logoff the user. Some systems that may have more limited capabilities may activate an operating system screen saver that is password protected after a period of system inactivity. In either case, the information that was displayed on the screen is no longer accessible to unauthorized users.

Sample questions for covered entities to consider:

- ✓ Do current information systems have an automatic logoff capability?
- ✓ Is the automatic logoff feature activated on all workstations with access to EPHI?

4. ENCRYTION AND DECRYPTION (A) - § 164.312(a)(2)(iv)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement a mechanism to encrypt and decrypt electronic protected health information."*

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (i.e., type of procedure or formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (i.e., translate) the text and convert it into plain, comprehensible text.

NOTE: The goal of encryption is to protect EPHI from being accessed and viewed by unauthorized users.

There are many different encryption methods and technologies to protect data from being accessed and viewed by unauthorized users.

Sample questions for covered entities to consider:

- ✓ Which EPHI should be encrypted and decrypted to prevent access by persons or software programs that have not been granted access rights?
- ✓ What encryption and decryption mechanisms are reasonable and appropriate to implement to prevent access to EPHI by persons or software programs that have not been granted access rights?

STANDARD § 164.312(b) Audit Controls

The next standard in the Technical Safeguards section is Audit Controls. This standard has no implementation specifications. The Audit Controls standard requires a covered entity to:

> *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."*

Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred.

It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use EPHI.

Sample questions for covered entities to consider:

- ✓ What audit control mechanisms are reasonable and appropriate to implement so as to record and examine activity in information systems that contain or use EPHI?
- ✓ What are the audit control capabilities of information systems with EPHI?
- ✓ Do the audit controls implemented allow the organization to adhere to policy and procedures developed to comply with the required implementation specification at § 164.308(a)(1)(ii)(D) for Information System Activity Review?

STANDARD § 164.312(c)(1) Integrity

The next standard in the Technical Safeguards section is Integrity. Integrity is defined in the Security Rule, at § 164.304, as *"the property that data or information have not been altered or destroyed in an unauthorized manner."* Protecting the integrity of EPHI is a primary goal of the Security Rule.

The Integrity standard requires a covered entity to:

> *"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."*

NOTE: The integrity of EPHI can be compromised by both technical and non-technical sources.

EPHI that is improperly altered or destroyed can result in clinical quality problems for a covered entity, including patient safety issues. The integrity of data can be compromised by both technical and non-technical sources. Workforce members or business associates may make accidental or intentional changes that improperly alter or destroy EPHI. Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures. The purpose of this standard is to establish and implement policies and procedures for protecting EPHI from being compromised regardless of the source.

There is one addressable implementation specification in the Integrity standard.

1. MECHANISM TO AUTHENTICATE ELECTRONIC PROTECTED HEALTH INFORMATION (A) - § 164.312(c)(2)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."*

In order to determine which electronic mechanisms to implement to ensure that EPHI is not altered or destroyed in an unauthorized manner, a covered entity must consider the various risks to the integrity of EPHI identified during the risk analysis. Once covered entities have identified risks to the integrity of their data, they must identify security measures that will reduce the risks.

Sample questions for covered entities to consider:

- ✓ Do existing information systems have available functions or processes that automatically check for data integrity such as check sum verification or digital signatures?
- ✓ Are electronic mechanisms to protect the integrity of EPHI currently used?

STANDARD § 164.312(d) Person or Entity Authentication

The Person or Entity Authentication standard has no implementation specifications. This standard requires a covered entity to:

> *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*

In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to EPHI. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:

NOTE: Authentication involves confirming that users are who they claim to be.

- ❑ Require something known only to that individual, such as a password or PIN.

- Require something that individuals possess, such as a smart card, a token, or a key.
- Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.

Most covered entities use one of the first two methods of authentication. Many small provider offices rely on a password or PIN to authenticate the user. If the authentication credentials entered into an information system match those stored in that system, the user is authenticated. Once properly authenticated, the user is granted the authorized access privileges to perform functions and access EPHI. Although the password is the most common way to obtain authentication to an information system and the easiest to establish, covered entities may want to explore other authentication methods.

Sample questions for covered entities to consider:

- ✓ What types of authentication mechanisms are currently used?
- ✓ What level or type of authentication is reasonable and appropriate for each information system with EPHI?
- ✓ Are other authentication methods available that may be reasonable and appropriate?

STANDARD § 164.312(e)(1) Transmission Security

The final standard listed in the Technical Safeguards section is Transmission Security. This standard requires a covered entity to:

> *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."*

In order to determine the technical security measures to implement to comply with this standard, covered entities must review the current methods used to transmit EPHI. For instance, is EPHI transmitted through email, over the Internet, or via some form of private or point-to-point network? Once the methods of transmission are reviewed, the covered entity must identify the available and appropriate means to protect EPHI as it is transmitted, select appropriate solutions,

and document its decisions. The Security Rule allows for EPHI to be sent over an electronic open network as long as it is adequately protected.

This standard has two implementation specifications:

1. Integrity Controls (Addressable)
2. Encryption (Addressable)

1. INTEGRITY CONTROLS (A) - § 164.312(e)(2)(i)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."*

Protecting the integrity of EPHI maintained in information systems was discussed previously in the Integrity standard. Integrity in this context is focused on making sure the EPHI is not improperly modified during transmission.

A primary method for protecting the integrity of EPHI being transmitted is through the use of network communications protocols. In general, these protocols, among other things, ensure that the data sent is the same as the data received.

There are other security measures that can provide integrity controls for EPHI being transmitted over an electronic communications network, such as data or message authentication codes, that a covered entity may want to consider.

NOTE: A covered entity should discuss reasonable and appropriate security measures to protect the integrity of EPHI during transmission with its IT professionals, vendors, business associates, and trading partners.

Sample questions for covered entities to consider:

- ✓ What security measures are currently used to protect EPHI during transmission?
- ✓ Has the risk analysis identified scenarios that may result in modification to EPHI by unauthorized sources during transmission?

- ✓ What security measures can be implemented to protect EPHI in transmission from unauthorized access?

2. ENCRYPTION (A) - § 164.312(e)(2)(ii)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."*

As previously described in the Access Control standard, encryption is a method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text. The Encryption implementation specification is addressable, similar to the addressable implementation specification at § 164.312(a)(2)(iv), which addresses Encryption and Decryption.

There are various types of encryption technology available to covered entities. For an encryption strategy to be successful, an organization must consider many factors. For example, for encryption technologies to work properly when data is being transmitted, both the sender and receiver must be using the same or compatible technology.

Covered entities use open networks such as the Internet and e-mail systems differently. Currently no single interoperable encryption solution for communicating over open networks exists. Adopting a single industry-wide encryption standard in the Security Rule would likely have placed too high a financial and technical burden on many covered entities. The Security Rule allows covered entities the flexibility to determine when, with whom, and what method of encryption to use.

NOTE: There are various types of encryption technology. To work properly, both the sender and the receiver must use the same or compatible technology.

A covered entity should discuss reasonable and appropriate security measures for the encryption of EPHI during transmission over electronic communications networks with its IT professionals, vendors, business associates, and trading partners.

Covered entities must consider the use of encryption for transmitting EPHI, particularly over the Internet. As business practices and technology change, situations may arise where EPHI being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis shows such risk to be significant, a covered entity must encrypt those transmissions under the addressable implementation specification for encryption.

Sample questions for covered entities to consider:

- ✓ How does the organization transmit EPHI?
- ✓ How often does the organization transmit EPHI?
- ✓ Based on the risk analysis, is encryption needed to protect EPHI during transmission?
- ✓ What methods of encryption will be used to protect the transmission of EPHI?

In Summary

The Security Rule Technical Safeguards are the technology and related policies and procedures that protect EPHI and control access to it. The Technical Safeguards standards apply to all EPHI. The Rule requires a covered entity to comply with the Technical Safeguards standards and provides the flexibility to covered entities to determine which technical security measures will be implemented.

Together with reasonable and appropriate Administrative and Physical Safeguards, successful implementation of the Technical Safeguards standards will help ensure that a covered entity will protect the confidentiality, integrity and availability of EPHI.

Resources

The remaining papers in this series will address other specific topics related to the Security Rule. The next paper in this series covers the final sections of the Security Rule, Organizational Requirements and Policies and Procedures and Documentation Requirements.

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)**

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

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)**

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

6 Basics of Risk Analysis and Risk Management

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, commonly known as the Security Rule. 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 sixth paper in the series is devoted to the required risk analysis and risk management 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

All electronic protected health information (EPHI) created, received, maintained or transmitted by a covered entity is subject to the Security Rule. Covered entities are required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. The Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities.

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 and Other Arrangements
- Requirements for Group Health Plans

POLICIES and PROCEDURES and DOCUMENTATION REQUIREMENTS

The objectives of this paper are to:

- Review the Security Rule required implementation specifications for Risk Analysis and Risk Management.
- Review the basic concepts involved in security risk analysis and risk management.
- Discuss the general steps involved in risk analysis and risk management.

Security Rule Requirements for Risk Analysis and Risk Management

The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to *"[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."* The Security Management Process standard has four required implementation specifications. Two of the implementation specifications are Risk Analysis and Risk Management.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, *"[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*

The required implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to *"[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)]."*

Both risk analysis and risk management are standard information security processes and are critical to a covered entity's Security Rule compliance efforts. As stated in the responses to public comment in the preamble to the Security Rule, risk analysis and risk management are important to covered entities since these processes will *"form the foundation upon which an entity's*

NOTE: Risk analysis and risk management serve as tools to develop and maintain a covered entity's strategy to protect the confidentiality, integrity, and availability of EPHI.

necessary security activities are built." (68 Fed. Reg. 8346.)

Much of the content included in this paper is adapted from government resources such as the National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems*. These government resources are freely available in the public domain.

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, *"Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations."*

The Security Rule does not prescribe a specific risk analysis or risk management methodology. This paper is not intended to be the definitive guidance on risk analysis and risk management. Rather, the goal of this paper is to present the main concepts of the risk analysis and risk management processes in an easy-to-understand manner. Performing risk analysis and risk management can be difficult due to the levels of detail and variations that are possible within different covered entities. Covered entities should focus on the overall concepts and steps presented in this paper to tailor an approach to the specific circumstances of their organization.

Important Definitions to Understand

NOTE: A risk analysis will identify potential threats to and vulnerabilities of information systems and the associated risk.

To better understand risk analysis and risk management processes, covered entities should be familiar with several important terms, including "vulnerability," "threat," and "risk," and the relationship between the three terms. These terms are not specifically defined in the Security Rule. The definitions in this paper are provided to put the Risk Analysis and Risk Management discussion in context. These definitions do not modify or update the Security Rule and are not inconsistent with the terms used in the Security Rule. Rather, the following definitions are consistent with common industry definitions and are from documented sources, such as NIST SP 800-30. Explanations of the terms are adapted from NIST SP 800-30 and are presented in the context of the Security Rule.

VULNERABILITY

Vulnerability is defined in NIST SP 800-30 as *"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised*

(accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as an inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and non-technical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

THREAT

An adapted definition of threat, from NIST SP 800-30, is "*[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.*"

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

- Natural threats may include floods, earthquakes, tornadoes, and landslides.
- Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- Environmental threats may include power failures, pollution, chemicals, and liquid leakage.

RISK

The definition of risk is clearer once threat and vulnerability are defined. An adapted definition of risk, from NIST SP 800-30, is:

"The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur. …[R]isks arise from legal liability or mission loss due to—

NOTE: A Vulnerability triggered or exploited by a Threat equals a Risk.

1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
2. Unintentional errors and omissions
3. IT disruptions due to natural or man-made disasters
4. Failure to exercise due care and diligence in the implementation and operation of the IT system."

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

NOTE: A threat must have the capability to trigger or exploit a vulnerability to create risk.

Example Risk Analysis and Risk Management Steps

There are numerous methods of performing risk analysis and risk management. There is no single method or "best practice" that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps. The following steps are provided as examples of steps covered entities could apply to their environment. The steps are adapted from the approach outlined in NIST SP 800-30.

EXAMPLE RISK ANALYSIS STEPS:

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation.

NOTE: CMS is not recommending that all covered entities follow this approach, but rather is providing it as a frame of reference.

EXAMPLE RISK MANAGEMENT STEPS:

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

When the following example risk analysis and risk management approaches contain actions that are required for compliance with the Security Rule, such as documentation, appropriate language and citations are used to highlight the Security Rule requirement. For example, the statement within these example approaches that a covered entity "must document" a certain action is a reference to the requirements of § 164.316(b)(1)(ii), the Documentation standard. These example approaches identify that a covered entity must or should perform certain actions, as required by the Security Rule, but does not require a covered entity to meet the requirements only by using the methods, steps, or actions identified in the example approach.

Example Risk Analysis Steps

As previously stated, the Security Rule requires covered entities to conduct an accurate and thorough risk analysis. This section of the paper provides an example approach to risk analysis which may be used by covered entities.

1. Identify the Scope of the Analysis

Risk analysis is not a concept exclusive to the healthcare industry or the Security Rule. Risk analysis is performed using different methods and scopes. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that a covered entity creates, receives, maintains, or transmits. This includes EPHI in all forms of electronic media. Electronic media is defined in § 160.103, as:

> *"(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission."*

Examples of Electronic Media with EPHI:
Hard drives, Floppy Disks, CDs, DVDs, Smart Cards, Personal Digital Assistants (PDA), Transmission Media, or Portable Electronic Storage Media.

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a covered entity's risk analysis

should take into account all of its EPHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its EPHI.

2. Gather Data

Once the scope of the risk analysis is identified, the covered entity should gather relevant data on EPHI. For example, a covered entity must identify where the EPHI is stored, received, maintained or transmitted. A covered entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods must be documented. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Many covered entities inventoried and performed an analysis of the use and disclosure of all protected health information (PHI) (which includes EPHI) as part of HIPAA Privacy Rule compliance, even though it was not a direct requirement. This type of inventory and analysis is a valuable input for the risk analysis.

The level of effort and resource commitment needed to complete the data gathering step depends on the covered entity's environment and amount of EPHI held. For example, a small provider that keeps its medical records on paper may be able to identify all EPHI within the organization by analyzing a single department which uses an information system to perform billing functions. In another covered entity with large amounts of EPHI, such as a health system, identification of all EPHI may require reviews of multiple physical locations, most (if not all) departments, multiple information systems, portable electronic media, and exchanges between business associates and vendors.

3. Identify and Document Potential Threats and Vulnerabilities

Once the covered entity has gathered and documented relevant data on EPHI, the next step is to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the EPHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining the level of risk.

The identification of threats and vulnerabilities could be separated into two distinct steps but are so closely related in the risk analysis process that they should be identified at the same time. Independent identification may result in large lists of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

IDENTIFY AND DOCUMENT THREATS

Covered entities must identify and document reasonably anticipated threats to EPHI. (See §§ 164.306(a)(2) and 164.316(b)(1)(ii).) To start, covered entities may compile a categorized list (such as natural, human, and environmental) of threats. Covered entities may identify different threats unique to the circumstances of their environment.

NOTE: A covered entity should focus its list of threats to those that are reasonably anticipated.

After the complete list is compiled, the covered entity should reduce the list to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, the geographic location of the entity will determine the natural threats that may create a risk. A hurricane is a threat, but a covered entity in Kansas probably would not consider it a reasonably anticipated threat due to its location. However, a covered entity in Kansas should consider the likelihood of a tornado a reasonably anticipated threat.

For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could target a covered entity and trigger or exploit vulnerabilities are employees (the most common source), ex-employees, hackers, commercial rivals, terrorists, criminals, general public, vendors, customers and visitors. Anyone that has the access, knowledge and/or motivation to cause an adverse impact on the covered entity can act as a threat.

Covered entities should analyze several information sources to help identify potential human threats to their systems. Information sources such as any history of system break-ins, security violation reports, and ongoing input from systems administrators, help desk personnel and the user community should be reviewed.

IDENTIFY AND DOCUMENT VULNERABILITIES

While identifying potential threats, covered entities must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk to EPHI. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).) The process of identifying vulnerabilities is similar to the process used for identifying threats. The entity should create a list of vulnerabilities, both technical and non-technical, associated with existing information systems and operations that involve EPHI.

There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports or security review reports. Sources of information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

The Internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories. These lists will be especially useful to large covered entities. In contrast, small covered entities will likely rely on their business associates for identification of system vulnerabilities, especially if their applications and information systems are maintained by outside vendors or contractors.

Another important way to identify technical vulnerabilities in information systems is through information systems security testing. The purpose of security testing is to assess the effectiveness of the security safeguards implemented to protect data, such as EPHI. There are many approaches to security testing. A common approach may involve developing a security testing and evaluation plan and to use security testing tools to scan workstations or the entire network (workstations and servers) for known technical vulnerabilities. The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

4. Assess Current Security Measures

The next step is to assess the current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to EPHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures can be both technical and non-technical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, automatic logoff and audit controls. Non-technical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability and responsibility, and physical and environmental security measures.

NOTE: Security measures can be both technical and non-technical.

Security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment. Small covered entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard EHPI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of EPHI in a small covered entity may differ from those that are appropriate in large covered entities.

The output of this step should be documentation of the security measures a covered entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly. (See §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

5. Determine the Likelihood of Threat Occurrence

Once the first four steps in the risk analysis process are complete, the covered entity has the information needed to determine 1) the likelihood that a threat will trigger or exploit a specific vulnerability and 2) the resulting impact on the covered entity. The next two steps (steps 5 and 6) use information gathered from the previous steps to help the covered entity make likelihood and impact determinations. The purpose of these steps is to assist the covered entity in determining the level of risk and prioritizing risk mitigation efforts.

"Likelihood of occurrence" is the probability that a threat will trigger or exploit a specific vulnerability. Covered entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Ratings such as high, medium and low or numeric representations of probability may be used to express the likelihood of occurrence. The ratings used will depend on the covered entity's approach. For example, a covered entity may choose to rate risks as high, medium and low, which could be defined as:

- High Likelihood – a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as the absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within a flood zone).

- Medium Likelihood – a moderate probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.

- Low Likelihood – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

6. Determine the Potential Impact of Threat Occurrence

If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. For covered entities, the most common outcomes include, but are not limited to:

- Unauthorized access to or disclosure of EPHI.
- Permanent loss or corruption of EPHI.
- Temporary loss or unavailability of EPHI.
- Loss of financial cash flow.
- Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI created, received, maintained, or transmitted by covered entities. The impact of potential outcomes, such as those listed above, should be measured to assist the covered entity in prioritizing risk mitigation activities.

Measuring the impact of a threat occurring in a covered entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow a covered entity to measure risk.

QUALITATIVE METHOD

The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale.

NOTE: Covered entities should consider the advantages and disadvantages of both qualitative and quantitative methods for determining the potential impact.

QUANTITATIVE METHOD

In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

A covered entity may use either method or a combination of the two methods to measure impact on the organization. Since there is no single correct method for measuring the impact during the risk analysis, a covered entity should consider the advantages and disadvantages of the two approaches.

The output of this step should be documentation of all potential impacts and ratings associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of EPHI within a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

7. Determine the Level of Risk

NOTE: Risk ranking will assist covered entities in prioritizing activities that must be performed.

Next, covered entities should determine the level of risk to EPHI. As discussed earlier, risk is a function determined by the likelihood of a given threat triggering or exploiting a specific vulnerability and the resulting impact. The covered entity will use the output of the previous two steps (steps 5 and 6) as inputs to this step. The output of those steps, likelihood and potential impact of threat occurrence data, will focus the covered entity's risk level determination to reasonably anticipated risks to EPHI.

The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

A risk level matrix can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a threat likelihood value of "high" combined with an impact value of "low" may equal a risk level of "low." Or a threat likelihood value of "medium" combined with an impact value of "medium" may equal a risk level of "medium."

Next, each risk level is labeled with a general action description to guide senior management decision making. The action description identifies the general timeline and type of response needed to reasonably and appropriately reduce the risk to acceptable levels. For example, a risk level of "high" could have an action description requiring immediate implementation of corrective measures to reduce the risk to a reasonable and appropriate level. Assigning action descriptions provides the covered entity additional information to prioritize risk management efforts.

One output of this step should be documented risk levels for all threat and vulnerability combinations identified during the risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

8. Identify Security Measures and Finalize Documentation

Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization's policies and procedures. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation.

This step only includes identification of security measures. The evaluation, prioritization, modification, and implementation of security measures identified in this step is part of the risk management process, addressed in the next section "Example Risk Management Steps."

NOTE: During the risk management process, recommended security measures will be evaluated, prioritized, modified, and implemented.

The final step in the risk analysis process is documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See § 164.316(b)(1)(ii).) A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process.

Example Risk Management Steps

Once the covered entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

1. Develop and Implement a Risk Management Plan

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the covered entity's evaluation, prioritization, and implementation of risk-reducing security measures.

For the risk management plan to be successful, key members of the covered entity's workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

The risk prioritization and mitigation decisions will be determined by answering questions such as:

- Should certain risks be addressed immediately or in the future?
- Which security measures should be implemented?

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the covered entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

- Risks (threat and vulnerability combinations) being addressed;
- Security measures selected to reduce the risks;
- Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the covered entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the covered entity's actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

2. Implement Security Measures

Once the risk management plan is developed, the covered entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the covered entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget. Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A covered entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the covered entity is responsible for its compliance with the Security Rule.

3. Evaluate and Maintain Security Measures

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

> *"Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 [(the Organizational Requirements)] and this subpart [(the Security Rule)] must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of [EPHI] as described at § 164.316."*

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

> "*Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [EPHI], that establishes the extent to which an entity's security polices and procedures meet the requirements of [the Security Rule].*"

For example, if the covered entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain EPHI, the potential risk to these devices must be analyzed to ensure the EPHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

In Summary

Risk analysis and risk management are the foundation of a covered entity's Security Rule compliance efforts. Risk analysis and risk management are on going processes that will provide the covered entity with a detailed understanding of the risks to EPHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

Resources

The previous papers in this series address specific requirements of the Security Rule. The final paper in this series will address implementation of Security Rule standards and implementation specifications in the small provider environment.

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)**