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 & Procedures, and Documentation Requirements
6. Basics of Risk Analysis & 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/hipaa/hipaa2***.

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 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 http://www.cms.hhs.gov/hipaa/hipaa2 for additional information and resources as they work through the security implementation process. There are many other sources of information available on the Internet. 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 http://www.cms.hhs.gov/hipaa/hipaa2 for the latest security papers, checklists, webcasts, and announcements of upcoming events.

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

Visit the Office for Civil Rights website, http://www.hhs.gov/ocr/hipaa, for the latest guidance, FAQs, 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)**