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)**