HIPAA Secure Now!

HIPAA Security and Omnibus Rules Overview

HIPAA Risk Assessment

The HIPAA Security Rule requires that a Risk Assessment be completed. The purpose of a Risk Assessment is to: identify where electronic protected health information (ePHI) is located, the threats to ePHI, the risks to ePHI and determine safeguards to better protect ePHI.

Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations." (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

RISK ANALYSIS (Required).
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 [organization].

Risk Assessment Methodology

1. Identify and document all ePHI repositories
2. Identify and document potential threats and vulnerabilities to each repository
3. Assess current security measures
4. Determine the likeliness of threat occurrence
5. Determine the potential impact of threat occurrence
6. Determine the level of risk
7. Determine additional security measures needed to lower level of risk
8. Document the findings of the Risk Assessment

Risk Management Process

A HIPAA Risk Assessment is part of the HIPAA Security Rule's Risk Management Process. Once a Risk Assessment is completed, the next step is implementing the recommendations from the Risk Assessment. This will further increase how an organization is protecting patient information.

Frequency

The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. Best practices are to perform a HIPAA Risk Assessment every year or when there are significant business or technology changes to an organization.

HIPAA Policies and Procedures

The HIPAA Security Rule requires that organizations have **written** policies and procedures on how to protect ePHI.

The HIPAA security policies and procedures are separate from the HIPAA privacy policies and procedures.

STANDARD
§ 164.316(b)(1) Documentation

> "(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 HIPAA Security Rule also requires that the policies and procedures be accessible to employees. An organization which has a single book of policies and procedures stored on a shelf is not providing the required ready access for employees.

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.

Policies Topics

HIPAA security policies and procedures address the administrative, technical and physical safeguards of the HIPAA Security Rule. Some topics include:

1. **Access to ePHI** ensure that employees only have access to ePHI and that access is limited to what they need to perform their job.
2. **Termination procedures** – ensure that access to ePHI is terminated when an employee is terminated.
3. **Encryption** – ensure that encryption is used on email that contain ePHI and that mobile devices that contain ePHI are encrypted.

HIPAA Security Training

The HIPAA Security Rule states that all employees that access ePHI need to have proper training on how to protect the information.

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

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

According to the HHS Security Standards: Administrative Safeguards:

> "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.

HIPAA Security Training Topics include:

1. **Malicious software** – employees need to understand the risks posed by viruses, malware and phishing scams, and how to avoid them.
2. **Login monitoring** – employees need to understand that all access to ePHI is recorded and reviewed.
3. **Passwords** – employees need to understand best password policies, not sharing password, etc.
4. **Social networks** – employees need to understand what should and shouldn't be posted on social networks (Facebook, Twitter, etc).

Periodic Security Reminders

The HIPAA Security Rule requires that employees not only receive HIPAA security training, but also receive periodic reminders on how to protect ePHI.

Business Associates

The HIPAA regulations define a "Business Associate" as:

> "A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Business Associates include:

- Information Technology (IT) companies
- Electronic Health Record (EHR) vendors
- Medical billing companies
- Law firms
- Accounting firms

The HIPAA Security Rule requires that covered entities (physician practices and hospitals) have written contracts or agreements with all Business Associates.

The HIPAA Omnibus Rule has expanded the HIPAA regulations to Business Associates:

> "Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.

New Business Associate Agreements

All existing Business Associate Agreements will need to be modified to contain the new HIPAA Omnibus Rule language.

Security Incident Response Procedures

The HIPAA Security Rule requires organizations to have a plan in place to address security incidents when they occur.

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

> "Implement policies and procedures to address 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.

Leon Rodriguez, director of the Office of Civil Rights (OCR) at the Department of Health and Human Services made it clear that organizations that act on security incidents will fare much better than those that don't.

> "One of the first things we look at is what did the entity do to analyze the root cause of the breach," he said. "[And] what did it do to remedy the root causes. Huge points for the entity that acts decisively to deal with those issues, to identify the reasons for the breach.

The HITECH Act of 2009 made security breach reporting a requirement. Depending on the type of breach and what was disclosed an organization may have to notify the following:

- Individuals / patients affected
- Health and Human Services (HHS)
- The Media

The HIPAA Omnibus Rule has made changes to the breach notification rule that put more onus on organizations to prove that ePHI has not been disclosed (basically an organization is guilty until it proves itself innocent). This will significantly increase the number of breach notifications that are sent to patients.

System Auditing and Review

The HIPAA Security Rule requires that all access to ePHI be logged and that the logs should be reviewed periodically to ensure that only proper access to ePHI is occurring.

§ 164.308(a)(1)(ii)(D) Information System Activity Review

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

It is important to periodically review system access logs to see if unauthorized access to ePHI is occurring. Unauthorized access may include:

- Access from external parties such as hackers.
- Access from employees which may include theft of ePHI or snooping through records in an EHR.

Some red flags that might point to unauthorized access include:

- Access to ePHI at 3am or after normal business hours.
- An employee accesses 75 records per day while other employees average only 10 records.

Employees should be reminded that all access to ePHI is recorded and that the logs are periodically reviewed for inappropriate activity.

An organization has to implement a system activity review process which makes sense for them. Reviewing on a daily basis might be too much work for some organizations. Some organizations review weekly or monthly and others periodically spot check system access logs.

Encryption

According to Wikipedia, encryption is:

> "is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can

Encryption is a "Safe Harbor" under the HIPAA Security Rule. That means if ePHI is encrypted and there is a security breach, there is no need to notify patients or HHS of the breach.

§ 164.312(a)(2)(iv) Encryption and Decryption

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.

HHS gives guidance that encryption should be used for data in transit and at rest. This means:

- **Data in transit** – ePHI sent via email or information accessed from a website
- **Data at rest** – data stored in an EHR or data stored on laptops or USB drives.

Encryption can be used for:

- Email
- Laptops
- USB drives
- DVD / CDs
- Smartphones (iPhones, Android, Windows phone, Blackberry)
- Tablets (iPads, etc.)

Contingency Plan

The HIPAA Security Rule requires that covered entities implement contingency plans to ensure access to ePHI.

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.

Contingency plans include:

- Data backup plan
- Disaster recovery plan

A **data backup plan** is required and critical to ensure that ePHI can be recovered if it is deleted or destroyed. Data backups should be encrypted and stored offsite (i.e. offsite backup).

A **disaster recovery plan** is required and critical in the event of a disaster (fire, flood, hurricane, etc.). A disaster recovery plan will allow covered entities to access ePHI in the event their primary computing infrastructure is damaged, destroyed or inaccessible.

Unique User Identification

The HIPAA Security Rule requires that individuals accessing ePHI use a unique identifier

§ 164.312(a)(2)(i) Unique User Identification

> "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.

User ids should not be shared with other employees. Passwords should not be shared or written down. Employees should protect their user id and passwords to ensure that only authorized access to ePHI is permitted.