Module 3: HIPAA Security Fundamentals
Module 3: Introduction

This module discusses:

• The three objectives of health information security—confidentiality, integrity, and availability

• The importance of ensuring that security objectives are met to protect the privacy of an individual’s health information

• Key Health Insurance Portability and Accountability Act (HIPAA) security-related concepts—including “scalable,” “flexible,” and “reasonable and appropriate”—as they relate to implementing safeguards to protect electronic protected health information (ePHI)
Module 3: Introduction (continued)

...this module discusses:

• Elements of the HIPAA Security Rule, including security standards and implementation specifications

• The importance of risk analysis

• The interrelationship between security and privacy
Module 3: Objectives

After completing this module, you will be able to:

• Discuss fundamental requirements of the HIPAA Security Rule

• Describe the HIPAA Security Rule standards and implementation specifications

• Explain how HIPAA Security Rule objectives and key concepts relate to building and evaluating a Security Rule compliance program

• Develop investigatory questions to apply to your case
Lesson 1: Objectives

After completing this lesson, you will be able to:

- Identify fundamental HIPAA Security Rule concepts to support the investigation of cases
- Analyze Security Rule’s requirements and implications for enforcement
Lesson 1: HIPAA Security Rule
Overview

Module 3

Topic 1: What is the HIPAA Security Rule? (continued)

The HIPAA Security Rule:

- Establishes a national set of security standards for ePHI
- Protects certain health information held or transmitted in electronic form by a HIPAA-covered entity
- Requires the administrative, physical, and technical safeguards that covered entities must put in place to secure individuals’ ePHI
- Does not apply to PHI transmitted orally or on paper
- Supports the Privacy Rule requirement to reasonably safeguard PHI in all forms
Topic 1: What is the HIPAA Security Rule? (continued)

...HIPAA Security Rule objectives:

- Protects against any reasonably anticipated threats and hazards to the confidentiality, integrity, or availability of ePHI
- Protects against any reasonably anticipated impermissible uses or disclosures
- Ensures compliance by the workforce
Topic 2: Achieving Health Information Security Objectives

The three cornerstones of the HIPAA security standards for ePHI are confidentiality, integrity, and availability (CIA).

- Confidentiality – means that ePHI is not made available or disclosed to unauthorized persons or processes
- Integrity – means that ePHI has not been altered or destroyed in an unauthorized manner
- Availability – means that ePHI is accessible and usable upon demand by an authorized person

Reference: 45 CFR § 164.304
Topic 3: HIPAA Security Rule Key Concepts

Understanding fundamental HIPAA Security Rule concepts will facilitate SAG investigation of HIPAA violations related to ePHI.

The majority of Security Rule violations investigated by HHS-OCR result from a covered entity not having adequate policies and procedures in place to safeguard ePHI contained on its information systems.
Topic 3: HIPAA Security Rule Key Concepts (continued)

Flexible and Scalable

The HIPAA Security Rule:

• Is scalable and flexible to allow covered entities to implement standards as appropriate for their circumstances

• Allows covered entities to tailor security policies, procedures, and technologies for safeguarding ePHI based on:
  – Size, complexity, and capabilities
  – Technical, hardware, and software infrastructure

References: 45 CFR §§ 164.306(b)(2), 164.306(e)
Topic 3: HIPAA Security Rule Key Concepts (continued)

Flexible and Scalable (continued)
• Allows covered entities to tailor security policies, procedures, and technologies for safeguarding ePHI based on:
  – Costs of security measures
  – Likelihood and possible impact of potential risks to ePHI
  – How security measures will be reviewed and modified to continue protecting ePHI in a changing environment

References: 45 CFR §§ 164.306(b)(2), 164.306(e)
Topic 3: HIPAA Security Rule Key Concepts (continued)

Reasonable and Appropriate

The Security Rule requires covered entities to:

- Evaluate risks and vulnerabilities in their environments
- Implement standards to protect against threats or vulnerabilities to ensure CIA of ePHI
- Select safeguards that are “reasonable and appropriate” given the covered entity’s analysis of risks

Failure to implement safeguards that effectively protect ePHI could result in violations of the Security Rule, which would be subject to SAG enforcement.
Topic 3: HIPAA Security Rule Key Concepts (continued)

**Threat**: the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threats that could impact the CIA of ePHI include:
- Natural threats
- Human threats
- Environmental threats

**Vulnerability**: 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.
Topic 3: HIPAA Security Rule Key Concepts (continued)

Risk

Risk is the likelihood of a given threat triggering or exploiting a particular vulnerability, and the resulting impact on the organization.

Risks to organizations can include compromised operations or legal liability due to:

• Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
• Unintentional errors or omissions
• IT disruptions due to natural or man-made disasters
• Failure to exercise due care and diligence in the implementation and operation of the IT system
Lesson 1: Knowledge Check

**Question 1:** What do the Security Rule concepts “scalable” and “flexible” mean for covered entities, and how does that affect enforcement of the HIPAA Security Rule?

**Question 2:** What does the Security Rule concept of “reasonable and appropriate” mean for covered entities, and how does that affect enforcement of the HIPAA Security Rule?
Lesson 1: Recap

The Security Rule requires covered entities to implement the Security Rule standards to ensure confidentiality, integrity, and availability of their information systems and ePHI.

The HIPAA Security Rule:

• Is scalable to fit to organizations of all sizes
• Is flexible so that covered entities and business associates can apply security measures appropriate for their environments
• Allows covered entities and business associates to implement safeguards that are “reasonable and appropriate” based on their analysis of risk
Lesson 2: HIPAA Security Rule
Lesson 2: Objectives

After completing this lesson, you will be able to:

• Differentiate between standards and implementation specifications

• Describe the three types of HIPAA Security Rule safeguards covered entities are required to implement to protect ePHI

• Explain the importance of ensuring that a covered entity has engaged in a risk analysis process when investigating compliance with the Security Rule

• Discuss the interrelationship of privacy and security
Topic 1: Security Standards and Implementation Specifications

All standards in the Security Rule are required. Many standards contain implementation specifications, which are:

- Detailed descriptions of methods or approaches for implementing security safeguards to meet a standard
- Either “required” or “addressable”

Reference: 45 CFR § 164.306(d)
Topic 2: Required vs. Addressable Implementation Specifications

“Required” implementation specifications:
- Must be implemented by all covered entities

“Addressable” implementation specifications:
- Are NOT optional
- May not be practical or achievable in all covered entity environments
- May be replaced with a “reasonable and appropriate” alternative that is equivalent, if necessary

Reference: 45 CFR §164.306
Topic 2: Required vs. Addressable Implementation Specifications (continued)

For example, the Access Control standard has four implementation specifications:

• **Required**
  – Unique User Identification (R)
  – Emergency Access Procedure (R)

• **Addressable**
  – Automatic Logoff (A)
  – Encryption and Decryption (A)
Topic 2: Required vs. Addressable Implementation Specifications (continued)

If the covered entity determines that an “addressable” implementation specification is NOT “reasonable or appropriate,” the Security Rule:

- Allows implementation of an equivalent safeguard that achieves the purpose of the standard
- Requires the covered entity to document why the safeguard was not “reasonable or appropriate”
- Requires the covered entity to document how the alternate safeguard is equivalent

Reference: 45 CFR §164.306 (d)
Topic 3: Administrative Safeguards

Administrative safeguards:

• Are administrative policies and procedures for protecting ePHI

• Include risk analysis and management, access management, workforce training, and evaluation of security measures

Reference: 45 CFR §§ 164.304, 164.308
### Topic 3: Administrative Safeguards (continued)

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>164.308(a)(1)</td>
<td>Risk Analysis (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Management (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sanction Policy (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information System Activity Review (R)</td>
</tr>
<tr>
<td>Assigned Security Responsibility</td>
<td>164.308(a)(2)</td>
<td>(R)</td>
</tr>
<tr>
<td>Workforce Security</td>
<td>164.308(a)(3)</td>
<td>Authorization and/or Supervision (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workforce Clearance Procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Termination Procedure (A)</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>164.308(a)(4)</td>
<td>Isolating Healthcare Clearinghouse Function (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Authorization (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Establishment and Modification (R)</td>
</tr>
<tr>
<td>Security Awareness Training</td>
<td>164.308(a)(5)</td>
<td>Security Reminders (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protection from Malicious Software (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log-in Monitoring (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password Management (A)</td>
</tr>
<tr>
<td>Security Incident Procedures</td>
<td>164.308(a)(6)</td>
<td>Response and Reporting (R)</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>164.308(a)(7)</td>
<td>Data Backup Plan (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disaster Recovery Plan (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency Mode Operation Plan (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Testing and Revision Procedure (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applications and Data Criticality Analysis (A)</td>
</tr>
<tr>
<td>Evaluation</td>
<td>164.308(a)(8)</td>
<td>(R)</td>
</tr>
<tr>
<td>Business Associate Contracts and Other Arrangements</td>
<td>164.308(b)(1)</td>
<td>Written Contract or Other Arrangement (R)</td>
</tr>
</tbody>
</table>
Topic 3: Administrative Safeguards (continued)

Security Management

The Security Management Process standard in the Security Rule requires covered entities to:

- Implement policies and procedures to prevent, detect, contain, and correct security violations
- Conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI

Reference: 45 CFR § 164.308(a)(1)
Topic 3: Administrative Safeguards (continued)

Risk Analysis

Risk analysis should be conducted as an ongoing process to:

• Aid in anticipating potential risks in a changing environment
• Track access to ePHI
• Identify new threats and vulnerabilities
• Detect security incidents

Reference: 45 CFR §164.308(a)(1)(ii)(A)
Topic 3: Administrative Safeguards (continued)

Risk Analysis (continued)

Questions that SAG could ask a covered entity during an investigation into a potential HIPAA security violation:

• Has the covered entity identified the ePHI it creates, receives, maintains, or transmits?

• What are the external sources of ePHI created, received, maintained, or transmitted by vendors or consultants?

• What are the human, natural, and environmental threats to information systems that contain ePHI?

Reference: 45 CFR §164.308(a)(1)(ii)(A)
Topic 3: Administrative Safeguards (continued)

Risk Management

Once the covered entity has completed the risk analysis, it must take any additional “reasonable and appropriate” steps required to:

• Implement security measures sufficient to reduce identified risks and vulnerabilities to a reasonable and appropriate level
• Ensure the confidentiality, integrity, and availability of all ePHI that the covered entity creates, receives, maintains, or transmits

References: 45 CFR §§ 164.306(a), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)
Topic 3: Administrative Safeguards (continued)

Risk Management (continued)

…it must take any additional “reasonable and appropriate” steps required to:

• Protect against any reasonably anticipated risks to the security or integrity of the information
• Protect against reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Rules
• Ensure compliance with the Privacy and Security Rules by its workforce

References: 45 CFR §§ 164.308(a)(1), 164.306(a), 164.308(a)(1)(ii)(A)
Topic 4: Physical Safeguards

Physical Safeguards:

• Are physical measures, policies, and procedures to safeguard a covered entity’s electronic information systems

• Safeguard buildings and equipment against natural and environmental hazards, and unauthorized intrusion
## Topic 4: Physical Safeguards (continued)

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Access Controls</td>
<td>164.310(a)(1)</td>
<td>Contingency Operations (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facility Security Plan (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control and Validation Process (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance Records (A)</td>
</tr>
<tr>
<td>Workstation Use</td>
<td>164.310(b)</td>
<td>(R)</td>
</tr>
<tr>
<td>Workstation Security</td>
<td>164.310(c)</td>
<td>(R)</td>
</tr>
<tr>
<td>Device and Media Controls</td>
<td>164.310(d)(1)</td>
<td>(R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disposal (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Media Re-use (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accountability (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Backup and Storage (A)</td>
</tr>
</tbody>
</table>
# Topic 5: Technical Safeguards

## Technical Safeguards (see Sec. 164.312)

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications (R) = Required, (A) = Addressable</th>
</tr>
</thead>
</table>
| Access Controls                   | 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)                                                                 |
Topic 5: Technical Safeguards (continued)

There are no specific requirements for what types of technology must be implemented to comply with the Security Rule’s technical safeguards, but a covered entity must consider and address each of the following:

- Access control
- Audit controls
- Integrity controls
- Person or entity authentication
- Transmission security
Encryption

Encryption is a technical mechanism that converts plain text into encoded text to prevent unauthorized access to ePHI.

The Security Rule includes two implementation specifications related to encryption. Both are addressable, but adopting encryption technologies will be reasonable and appropriate for many covered entities.
Activity 3: Which Safeguard Could Have Prevented This?

Working in your Table Group, read your assigned scenario and refer to the safeguards of the Security Rule, 45 CFR §§ 164.308, 164.310 and 164.312 located on pages 6, 9 and 11, respectively, of your Appendix, to answer the discussion questions; then provide your answer during the class review.

Discussion Questions:

Based on your scenario, identify which specific safeguards might have prevented the incident in your scenario:

1. Administrative safeguards?
2. Physical safeguards?
3. Technical safeguards?
Topic 6: Interrelationship Between Privacy and Security

The HIPAA Security Rule complements the HIPAA Privacy Rule:

- Security requirements include a set of tools for ensuring compliance with the Privacy Rule as well as the Security Rule
- The Security Rule provides detailed requirements, which protect only ePHI
- The Privacy Rule safeguards provision, 45 CFR § 164.530(c), is more general and protects the privacy of all PHI, not just ePHI
Topic 6: Interrelationship Between Privacy and Security (continued)

Analogous Requirements of Both Rules

Both Rules require covered entities to:

• Implement policies
• Ensure accountability for compliance
• Limit access to PHI
• Conduct workforce training
• Safeguard PHI
Topic 7: Investigating Potential HIPAA Security Rule Violations

Investigation Questions

Key items to look for during an investigation include:

- Was the ePHI used or disclosed? By or to whom?
- What documentation regarding the use and disclosure was maintained?
- Were the other administrative requirements followed?
- Were individual rights protected?
- Were the requirements of the Security Rule met?

Answers to these questions may lead an investigator to determine that multiple violations exist.
Lesson 2: Knowledge Check

**Question 1:** What are administrative safeguards?

**Question 2:** If a Security Rule implementation specification is “addressable,” the covered entity may identify a “reasonable and appropriate” alternative under what conditions?

**Question 3:** What key information might the SAG need during an investigation into a potential HIPAA security violation?

**Question 4:** What should be a critical first step in a covered entity’s compliance efforts?

**Question 5:** What are some comparable requirements of both the HIPAA Privacy and Security Rules?
Lesson 2: Recap

The HIPAA Security Rule requires three types of safeguards—administrative, physical, and technical.

Covered entities are required to implement specific safeguards to meet the requirements of each security standard to protect their information systems and the ePHI they contain against threats and vulnerabilities, and to prevent unauthorized access to or disclosure of ePHI.
Module 3: Recap

This module discussed:

• The three objectives of the HIPAA Security Rule—confidentiality, integrity, and availability

• The importance of ensuring that security objectives are met to protect the privacy of an individual’s health information

• The importance of conducting risk analysis as a critical first step in implementing a security compliance program
Module 3: Recap (continued)

...this module discussed:

- HIPAA security-related key concepts, including “scalable,” “flexible,” and “reasonable and appropriate” as they relate to implementing safeguards to protect ePHI

- Elements of the HIPAA Security Rule, including security standards and implementation specifications

- The interrelationship between security and privacy
Module 3: Summary

Having completed this module, you are able to:

• Discuss fundamental requirements of the HIPAA Security Rule
• Describe the HIPAA Security Rule standards and implementation specifications
• Explain how HIPAA Security Rule objectives and key concepts relate to building and evaluating a Security Rule compliance program
• Develop investigatory questions to apply to your case