Module 1: State Attorneys General
Enforcement of Federal Health Privacy Law
Module 1: Introduction

This module of the HIPAA Enforcement Training for State Attorneys General (SAG) provides an overview of:

• ARRA/ HITECH’s impact on SAG
• HIPAA rules and terminology
• Identifying potential HIPAA violations
• Investigating potential HIPAA violations
Module 1: Objectives

After completing this module, you will be able to:

• Discuss your authority under ARRA/HITECH
• Define terminology and the premise of the Privacy Rule
• Explain the purpose of the Security Rule
• Identify potential HIPAA violations and your role in investigating alleged violations
Lesson 1: Objectives

After completing this lesson, you will be able to:

• Describe SAG authority for enforcement of HIPAA under ARRA/HITECH

• Discuss the effect of ARRA/HITECH on how HIPAA applies to business associates and breach notifications
Topic 1: Overview of ARRA/HITECH Requirements

ARRA addresses health information technology:

- Title XIII and Title IV of Division B are known as the Health Information Technology for Economic and Clinical Health (HITECH) Act
- Subtitle D of HITECH addresses health information privacy
- Effective Date: February 17, 2009
Topic 2: Overview of SAG Role in HIPAA Enforcement Under ARRA/HITECH

- Subtitle D § 13410 - Improved Enforcement
- SAG may bring civil actions for alleged violations of HIPAA Privacy and Security on behalf of state residents
- ARRA/HITECH instituted federal breach notification requirements
- Extended liability under HIPAA Rules to Business Associates of Covered Entities
Topic 3: SAG HIPAA Enforcement Action

Activity 1: State of Connecticut case

- Take about 10 minutes to read paragraphs I-IV
- Located on page 1 of your Appendix
- Keep in mind the various elements
Lesson 2: Objectives

After completing this lesson, you will be able to:

• Describe the HIPAA statute and regulations

• Explain the purpose and function of the HIPAA Privacy Rule

• Discuss the purpose and function of the HIPAA Security Rule
Topic 1 Overview

Topic 1 will address these questions:

• Why HIPAA
• What is HIPAA
• Who is regulated and protected
• What information
• How – rule making
Topic 1: Why HIPAA?

• The potential consequences of not protecting privacy or security can be severe

• In 1996, Congress passed HIPAA, which includes provisions calling for privacy and security protections
Topic 2: What is HIPAA?
Topic 2: What is HIPAA? (continued)

Title II: Subtitle F – Administrative Simplification

• Encourages efficiencies in exchange of health information

• Requires HHS to adopt standards for electronic transmission of certain health information

Title II, Subtitle F, Section 264, *Recommendations with Respect to Privacy of Certain Health Information*:

• Requires Secretary of HHS to establish standards with respect to privacy of individually identifiable health information if Congress does not do so in 3 years
Topic 2: What is HIPAA? (continued)
Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification
Topic 2: What is HIPAA? (continued)

Standard Transactions:

- Health care claims or equivalent encounter information
- Referral certification and authorization
- Health care claim status
- Health care payment and remittance advice
- Eligibility for a health plan
- Enrollment and disenrollment in a health plan
- Health plan premium payments
- Coordination of benefits

Reference: 45 CFR § 162.1101
Topic 3: HIPAA Rules

Covered Entities

A covered entity is:

- A health plan
- A health care clearinghouse
- A health care provider who transmits any health information in electronic form in connection with a covered transaction—one for which the HHS Secretary has adopted standards

Examples:

- Requesting payment
- Inquiring regarding the status of a health care claim

Reference: 45 CFR §160.103
Topic 3: HIPAA Rules (continued)

More Information on Health Plans

A Health Plan includes:

- Health insurance companies
- Health Maintenance Organizations (HMOs)
- Group health plans
  (e.g. employer-sponsored health plans)
- Government programs that pay for health care:
  - Medicare & Medicaid
  - Military & veterans health care programs
Topic 3: HIPAA Rules (continued)

More Information on Health Care Clearinghouses

Health care clearinghouses:

- Receive health information from other entities
- Process or facilitate the processing of health information to or from non-standard formats to or from standard formats
Topic 3: HIPAA Rules (continued)

Individually Identifiable Health Information (IIHI)

As defined in HIPAA & the Privacy Rule, IIHI is:

Health information (including demographic information collected from an individual) if it is created or received by a health care provider, health plan, employer, or health care clearinghouse...
Topic 3: HIPAA Rules (continued)

Individually Identifiable Health Information (IIHI) (continued)

...and relates to the:

- Past, present, or future physical or mental health or condition of an individual
- Provision of health care to an individual
- Past, present, or future payment for the provision of health care to an individual
Topic 3: HIPAA Rules (continued)

Individually Identifiable Health Information (IIHI) (continued)

Information categorized as IIHI must also satisfy the criteria of identifying the individual or providing a reasonable basis to believe it can be used to identify the individual.

A patient’s name, contact information, and account numbers are generally considered to be individual identifiers and if created or received by a covered entity would be IIHI.

Reference: 45 CFR § 160.103
Lesson 2: HIPAA Overview

Module 1

Topic 3: HIPAA Rules (continued)

Protected Health Information (PHI)

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of electronic media at 45 CFR § 160.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.
Topic 3: HIPAA Rules (continued)

Protected Health Information (PHI) (continued)

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; and records described at 20 U.S.C. 1232g(a)(4)(B)(iv)

(ii) Employment records held by covered entities in their role as employer

Reference: 45 CFR §160.103
Topic 3: HIPAA Rules (continued)

Examples of PHI

- Medical records of patients that visit a covered provider’s office
- Billing records
- Other records that contain enough information to identify the individual

Reference: 45 CFR § 160.103
Lesson 2: HIPAA Overview

Module 1

Topic 3: HIPAA Rules (continued)

Electronic Protected Health Information (ePHI)

ePHI is protected health information that is maintained in, or transmitted in electronic media by a covered entity.
Topic 3: HIPAA Rules (continued)

Business Associates

- A business associate is a person or entity that performs a function or activity on behalf of a covered entity, or provides certain services to a covered entity that involve the use or disclosure of PHI
- Covered entities are generally required to execute a written contract or other written agreement/arrangement with each of their business associates
Topic 3: HIPAA Rules (continued)

Business Associates (continued)

Business associates include individuals or organizations that conduct:

- Legal services
- Accounting services
- Claims processing or administration
- Data analysis
- Utilization review
- Quality assurance
- Billing
- Benefits management
- Practice management
- Repricing
Topic 3: HIPAA Rules (continued)

Business Associates (continued)

• Not every entity that a covered entity does business with is a business associate:
  – A member of the covered entity’s workforce is not a business associate
  – A conduit of PHI (e.g., U.S. Postal Service or a messenger service) is not a business associate

• A covered entity can be a business associate of another covered entity

Reference: 45 CFR § 160.103
Topic 4: HIPAA Privacy Rule

Privacy Rule

Full citation:

“Standards for the Privacy of Individually Identifiable Health Information; Final Rule.”
65 Federal Register (FR) 82462 (December 28, 2000)
Topic 4: HIPAA Privacy Rule (continued)

Privacy Rule (continued)

Modified by:

• “Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information,” 65 FR 82944 (December 29, 2000)

• “Standards for Privacy of Individually Identifiable Health Information,” 67 FR 53182 (August 14, 2002)


• “HIPAA Administrative Simplification: Enforcement,” 71 FR 8390 (February 16, 2006)

• “HIPAA Administrative Simplification: Enforcement,” 74 FR 56123 (October, 30, 2009)
Topic 4: HIPAA Privacy Rule (continued)

Privacy Rule (continued)

Incorporated at:

• 45 Code of Federal Regulations (CFR), Part 160 – Includes definitions, preemption provisions, compliance and investigations, imposition of civil money penalties and procedures for hearings for all Administrative Simplification provisions

• 45 CFR, Part 164, titled “Security and Privacy”

• Subpart A – Includes general provisions, such as definitions that apply to both the Privacy and Security Rules
Lesson 2: HIPAA Overview

Topic 4: HIPAA Privacy Rule (continued)

Privacy Rule (continued)

45 CFR, Part 164, titled “Security and Privacy”

- Subpart E, among other things:
  - Establishes standards for use and disclosure of PHI by covered entities
  - Establishes individuals’ rights with regard to their PHI
  - Sets out general rule that covered entities/business associates may only use and disclose PHI as permitted or required by the HIPAA Privacy Rule
  - Provides standards explaining permitted and required uses and disclosures
  - Outlines administrative requirements for covered entities
Topic 5: HIPAA Security Rule

Security Rule

Full citation:


Incorporated at:

• 45 CFR, Part 160, and Subpart C of Part 164
Topic 5: HIPAA Security Rule (continued)

Security Rule (continued)

45 CFR, Part 164, Subparts A and C:

- Address security standards and implementation specifications to protect electronic PHI (ePHI) from unauthorized disclosure or access

- Define three types of safeguards that covered entities are required to have in place to protect ePHI:
  - Administrative
  - Physical
  - Technical
Lesson 2: Recap

Health Insurance Portability and Accountability Act:

• Title I – HIPAA provides protection against loss of health insurance due to job loss ("portability") and addresses fraud and abuse.

• Title II - Establishes standards for transmission of electronic health information
  – Subtitle F - Recommendations for protection of the privacy of health information
Lesson 2: Recap (continued)

Privacy Rule

• Establishes standards for covered entities to protect PHI

• Establishes individuals’ rights with regard to their PHI

Security Rule

• Establishes security safeguards covered entities are required to have in place to protect ePHI from unauthorized access or disclosure
Lesson 3: Identifying Potential HIPAA Violations
Lesson 3: Objectives

After completing this lesson, you will be able to:

• Discuss how to identify potential HIPAA violations
• Describe what constitutes a violation of the HIPAA Rules
• Recognize whether or not other cases under SAG investigation may also raise issues under the HIPAA Rules
Topic 1: Identifying Potential HIPAA Violations

How SAG may learn about violations of HIPAA:

- Monitor local news outlets
- Receive complaints directly
- Whistleblowers
- Referred cases from other agencies
Topic 2: Events and Conditions Constituting HIPAA Violations

Inappropriate use or disclosure:

• May be the first indicator of a HIPAA Privacy or Security Rule violation

• Not required for proving the existence of a HIPAA Privacy or Security Rule violation

• Upon investigation, further HIPAA Privacy or Security violations may be present
Topic 2: Events and Conditions Constituting HIPAA Violations (continued)

Once a violation is suspected or detected, a SAG investigator will want to determine what provision or provisions of the Rules were violated.

Investigators should keep in mind that the HIPAA Rule requires documentation of the covered entity’s policies and procedures for all standards.

Investigators can look at both whether the policies and procedures met the requirements of the Rules and whether the policies and procedures themselves were followed. Also consider whether or not other related standards may be implicated.
Lesson 3: Identifying Potential HIPAA Violations

Module 1

Topic 3: Determining Whether Other Investigations by SAG May Have HIPAA Implications

May uncover violations of HIPAA by re-examining existing cases.

Examples:

• Health care fraud
• Labor and employment
• Adherence to state laws involving health care access and licensure
Lesson 3: Recap

Local new stories, residents’ complaints, or current civil or criminal caseloads may reveal a HIPAA violation.

A public exposure of PHI may sometimes, but not always, indicate a failure to comply with the HIPAA Privacy and Security Rules.
Lesson 4: Investigating Potential HIPAA Violations
Lesson 4: Objectives

After completing this lesson, you will be able to:

• Recognize when multiple violations of HIPAA result from a single incident

• Describe the interrelationship of violations of the Privacy and Security Rules
Topic 1: Multiple Violations Resulting from Single Incidents or Programs

Multiple violations of the various aspects of the Privacy Rule could be uncovered during the investigation of one incident.
Topic 2: Relationship of Security Violations to Privacy Violations

• A violation of the Security Rule can lead to a violation of the Privacy Rule
• If confidentiality is not protected, privacy can be violated
Module 1: Knowledge Check

Question 1: Which Act extends enforcement of HIPAA to SAG?

Question 2: What rule says that PHI may be used or disclosed for certain purposes?

Question 3: What must covered entities have in place to protect PHI?

Question 4: What are some ways that you might learn of HIPAA violations in your state?
Module 1: Recap

- ARRA/HITECH gave authority to SAG for HIPAA enforcement at the state level
- ARRA/HITECH established new breach notification requirements
- ARRA/HITECH extended the Privacy and Security Rules to business associates of covered entities
- HIPAA Title II, Subtitle F, required the Secretary of HHS to establish security standards, and health privacy standards if Congress did not do so
- The result was the Privacy and Security Rules, which apply to covered entities
Module 1: Recap (continued)

• News reports may reveal potential HIPAA violations due to a breach
• An investigator may establish a fact pattern by determining what requirements were not met
• An investigation may reveal multiple violations of both the Privacy Rule and Security Rule
Module 1: Summary

Having completed this module, you are able to:

• Discuss your authority under ARRA/HITECH
• Define terminology and the premise of the Privacy Rule
• Explain the purpose of the Security Rule
• Identify potential HIPAA violations and your role in investigating alleged violations