Module 4: Introduction

This module provides detail on:

- The Health Information Technology for Economic and Clinical Health (HITECH) Act, Division A, Title XIII, Subtitle D of the American Recovery and Reinvestment Act (ARRA) of 2009
- The role of State Attorneys General (SAG) under ARRA/HITECH
- Application of the Privacy and Security Rules to business associates under ARRA/HITECH
- Other provisions related to HIPAA under ARRA/HITECH
Module 4: Objectives

After completing this module, you will be able to:

• Discuss your authority to enforce HIPAA

• Describe the civil money penalty (CMP) structure established under ARRA/HITECH

• Discuss the application of Privacy and Security provisions to business associates under ARRA/HITECH

• Summarize the breach notification requirements established by ARRA/HITECH

• Discuss other provisions related to HIPAA under ARRA/HITECH
Lesson 1: Overview of ARRA/HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act:

- Enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009
- Signed into law on February 17, 2009
- Enhances enforcement of the HIPAA regulations
- Gives enforcement authority to SAG to protect state residents whose HIPAA protections or rights have been violated
Lesson 2: A New Role for SAG in HIPAA Enforcement

Section 13410(e), “Enforcement Through State Attorneys General,” of ARRA/HITECH gives authority to SAG to bring a civil action on behalf of state residents that have been or are threatened or adversely affected by any covered entity or business associate that violates HIPAA requirements.

Amends Section 1176 of the Social Security Act (42 USC 1320d-5)
Lesson 3: Increased Civil Money Penalties (CMP)

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Identical Violations per Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For violations occurring before</td>
<td>For violations occurring on or after</td>
</tr>
<tr>
<td>(A) Did Not Know</td>
<td>Up to $100</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>Up to $100</td>
<td>$1,000 - $50,000</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect-Corrected</td>
<td>Up to $100</td>
<td>$10,000 - $50,000</td>
</tr>
<tr>
<td>(C)(ii) Willful Neglect-Not Corrected</td>
<td>Up to $100</td>
<td>$50,000</td>
</tr>
</tbody>
</table>

Section 13410(d) of the HITECH Act revised section 1176(a) of the Social Security Act ("the Act") by establishing a tiered increase in CMP, including:

- Four categories of violations that reflect increasing levels of culpability
- Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation
- A maximum penalty amount of $1.5 million for all violations of an identical provision
Lesson 4: Periodic Audits

Section 13411 states that the Secretary of Health and Human Services (HHS) shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of the HIPAA Privacy and Security Rules comply with the requirements.
Lesson 5: Clarification of Wrongful Disclosures Criminal Penalties

Section 13409 amends Section 1177(a) of the Social Security Act to state that a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of HIPAA if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1180(b)(3)) and the individual obtained or disclosed such information without authorization.

Reference: 42 U.S.C. 1320d-6(a)
Lesson 6: Effective Date

HITECH, Section 13410 (“Improved Enforcement”); Subsection (e), (Enforcement through State Attorneys General); Subsection (3) (“Effective Date”):

SAG may pursue damages for violations of the Privacy and Security Rules that occur after February 17, 2009. However, the effective date of most HITECH provisions is February 17, 2010, unless otherwise specified in the statute.
Lesson 7: Application of Privacy and Security Provisions to Business Associates

Sections 13401 and 13404 of the HITECH Act:

Extend to business associates certain of the same requirements of the HIPAA Rules that apply to covered entities.
Lesson 7: Application of Privacy and Security Provisions to Business Associates (continued)

Sections 13401 and 13404 of the HITECH Act:

• Require business associates to comply with most provisions in the Security Rule, and with the Privacy Rule’s limitations on the use and disclosure of PHI

• Require the business associate agreement (e.g., contract) between a covered entity and its business associate to incorporate the relevant HIPAA Privacy Rule requirements

• Apply civil and criminal penalties to a business associate in the same manner they are applied to a covered entity that violates the HIPAA Privacy or Security Rules
Lesson 8: Business Associate Contracts Required for Certain Entities

Section 13408 states that each organization that:

• Provides data transmission of protected health information (PHI) to a covered entity or its business associate, and
• Requires routine access to the PHI

...must enter into a business associate contract and shall be treated as a business associate of the covered entity under the HIPAA Privacy and Security Rules.
Lesson 9: Breach Notification Requirements

Section 13402 of the HITECH Act requires covered entities to notify each affected individual, HHS, and in some cases the media of a breach of “unsecured PHI.”

Office for Civil Rights (OCR) issued, in August 2009, an interim final rule for breach notification requirements, which are enforceable by OCR and SAG.
Lesson 9: Breach Notification Requirements (continued)

“Unsecured PHI” is defined as PHI that is not secured through the use of a technology or methodology specified by HHS’ Breach Notification Guidance.

• Titled “Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.”

The guidance identifies encryption and destruction as the accepted methods for securing PHI.
Lesson 9: Breach Notification Requirements (continued)

Notification of a breach of unsecured PHI:

• Is required within 60 days after discovery of the breach, unless delay is requested by law enforcement

• A breach is considered “discovered” by a covered entity or by a business associate as of the first day on which the breach is or should reasonably have been known to have occurred
Lesson 9: Breach Notification Requirements (continued)

Notification of a breach of unsecured PHI:

- Business associates must notify the covered entity of a breach, and in some cases may be required by the covered entity to notify affected individuals.

- Is sent in paper form by first class mail to the last known address of the individual or his/her next of kin, unless preference is specified by the individual for electronic mail.
Lesson 9: Breach Notification Requirements (continued)

Breach involving less than 500 individuals:

- Notice to affected individuals
- Notice to HHS. A covered entity may maintain a log and submit it annually to the Secretary of HHS
Lesson 9: Breach Notification Requirements (continued)

Breach involving more individuals:

- Notice to affected individuals
- Contemporaneous notice to the Secretary of HHS for posting to the HHS public website (if 500 or more individuals affected)
- Notice to prominent media within the state or jurisdiction (if more than 500 individuals affected)
Lesson 10: Other Provisions

HITECH provides for additional provisions:

• Requested Restrictions on Certain Disclosures
• Accounting of Certain PHI Disclosures if the Covered Entity Uses Electronic Health Records
• Prohibition on the Sale of PHI and ePHI
• Access in Electronic Format
• Education on Health Information Privacy
• Conditions on Certain Contacts as Part of Health Care Operations – Marketing
• Conditions on Certain Contacts as Part of Health Care Operations – Fundraising
Module 4: Recap

Under ARRA/HITECH:

- HIPAA enforcement authority was granted to SAG
- A tiered increase in CMP was established
- The HIPAA Rules apply to business associates in much the same way they do to covered entities
- Breach notifications must be sent to affected individuals, the Secretary of HHS, and in some cases the media
- New limitations are implemented related to individually requested restrictions on disclosures, sale of PHI, and marketing communications
- Widened application of criminal penalties to business associates, employees of covered entities
Module 4: Summary

Having completed this module, you are able to:

• Discuss your authority to enforce HIPAA

• Describe the civil money penalty (CMP) structure established under ARRA/HITECH

• Discuss the application of Privacy and Security provisions to business associates under ARRA/HITECH

• Summarize the breach notification requirements established by ARRA/HITECH

• Discuss other provisions related to HIPAA under ARRA/HITECH