ARRA’s HITECH Amendments to HIPAA Privacy & Security Rules

John Hickman
Alston & Bird, LLP
jhickman@alston.com

Amended HIPAA Privacy and Security Rules

■ HIPAA Amendments are in The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of The American Recovery & Reinvestment Act of 2009 (ARRA).

■ Effective Date: February 17, 2010, except as otherwise noted.
  ■ HITECH Breach requirements effective September 23, 2009 (enforcement moratorium until approximately February 23, 2010)
Overview of Amendments to HIPAA Privacy and Security Rules

- Expanded Obligations of Business Associates (BAs)
  - Security
  - Privacy
- Affirmative Notification of Breach Requirements
  - New rules effective September 23, 2009
- Guidance on “Minimum Necessary” Standard
- Prohibition on Sale of PHI
- Restrictions on Marketing
- Application to Personal Health Records (PHR) Vendors
  - FTC Enforcement
- Increased Enforcement and Penalties, including application to BAs

Note: This presentation relates primarily to obligations of employer-sponsored health plans, not health care providers to which additional requirements apply.

Expanded Obligations of Business Associates (BAs)

- Pre-ARRA Rule:
  - BAs were not directly subject to the HIPAA Privacy and Security Rules. Rather, their duties arose out of their BA Agreements.
- Revise BAAs to incorporate expanded Privacy and Security Rule obligations.
- Civil and criminal penalties now apply directly to BAs.
Expanded Obligations of BAs (con’t)

- Expanded Security Rule Obligations:
  - Security Rule obligations that govern Administrative, Physical and Technical Safeguards, and require Security Policies and Procedures, now apply directly to BAs.
  - BAs are also directly subject to additional ARRA requirements, which must be incorporated into BA Agreements.

Expanded Requirements for BAs

- Most security requirements to apply directly to BAs
  - Pre-ARRA—security requirements not directly imposed on BAs
    - BA only contractually obligated to CE to safeguard ePHI
  - Post-ARRA—effective Feb. 17, 2010, most HIPAA security requirements apply directly to BAs
    - Establish administrative safeguards to protect ePHI
    - Implement physical safeguards to limit physical access to ePHI
    - Implement technical safeguards for electronic information systems that control access to ePHI
    - Implement reasonable and appropriate policies and procedures and maintain proper documentation
### HIPAA Security Standards at a Glance

#### Physical Safeguards
- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

#### Technical Safeguards
- Access controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

#### Administrative Safeguards
- Security Management Processes
- Assigned Security Responsibility
- Workforce Security
- Information Management Access
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

#### Organizational Requirements
- Business Associate Contracts and Other Arrangements
- Requirements for Group Health Plans

#### Policies and Procedures and Documentation Requirements
- Policies and Procedures
- Documentation

### Administrative Safeguards – Questions to Ask

- **Risk Management** – Has TPA conducted an assessment of potential risks and vulnerabilities to its ePHI. This process must be ongoing and safeguards must be periodically re-evaluated.

- **Security Policies and Procedures** – Does TPA have policies and procedures to prevent, detect, contain, and correct violations of HIPAA’s security requirements; TPA must ensure that the “workforce” has been authorized and has appropriate access to ePHI, and otherwise meets HIPAA’s security requirements.

- **HIPAA Security Official** – Has TPA identified a person responsible for developing and implementing the security policies and procedures.

- **Security Incidents** – TPA must have procedures to report suspected or actual breaches involving ePHI.

- **Sanction Policy** – Appropriate sanctions must be taken against members of the “workforce” who fail to comply with the policies and procedures.

- **Security Awareness Training** – Ongoing training must be provided for “workforce” on HIPAA security responsibilities.
Physical Safeguards

- Facility Security
  - Does TPA office building security protect the areas where ePHI is stored or used.
  - Question those in your area who do not have ID badges.
  - Visitors must be escorted.

- Media and Hardcopy Controls
  - Do not leave PHI unattended on desks, copy machines, printers, or faxes, or in other locations that are easily accessible by unauthorized personnel or visitors.
  - Lock PHI (hardcopy, CDs, floppy disks) in file cabinets and desk drawers during non-working hours.
  - Ensure that hardcopies and electronic storage media that contain PHI are properly destroyed when no longer needed (i.e., shred paper, and have a process to destroy media).

Physical Safeguards (continued)

- Workstation Security
  - Logoff or lock your PC when you leave your desk and at the end of each day.
  - Encrypt hard drives on laptops and when traveling with a laptop, never check it in with your luggage, be sure you carry it with you. Also, physically lock up laptops while offsite or in a hotel or use security cables.
  - Make sure any critical data on a PC or laptop is backed up frequently to the network.
  - For home systems, ensure that necessary technical safeguards, such as firewall and virus protection.
Technical Safeguards

- **Password Management**
  - Each person must only use his/her own userID and protect it as private. If you need access to someone else’s system or data, your supervisor must approve the request.
  - Choose a strong password, minimum of 8 characters.
    - Do not use dictionary words.
    - Combine with upper, lower case letters, numbers and special characters (ex. bigsc00p, two words together, replace the letter O with zeros).
  - Change your password every 90 days or if suspected of compromise.
  - Call the IT specialist if you suspect someone has used your ID (ex., if your password doesn’t work).

Technical Safeguards (continued)

- **Malicious Code (Virus) Protection**
  - Always keep your anti-virus software enabled. Do not manually stop it from running its scheduled update process.
  - Don’t open email or email attachments from unknown individuals as they may contact viruses.
  - Avoid downloading software from the Internet. It may contain viruses or spyware, which can be used to steal your personal or company data from your PC.
  - Contact IT if you suspect your computer has a virus.

- **Encryption**
  - ePHI information requires additional safeguards before it is transmitted to a 3rd party.
    - Encryption scrambles the data that makes up a file, and requires a password to unencrypt the data.
    - By default, email sent via the Internet is not secured or encrypted. So do not send ePHI as email attachments.
Expanded Privacy Obligations

- Expanded Privacy Rule Obligations:
  - Statutory requirement that BAs may only use and disclose PHI in accordance with the BA Agreement requirements.
  - BA is directly subject to additional Privacy Rule requirements under ARRA.
  - If BA knows of material breach by Covered Entity (CE), BA is obligated to (1) take action to cure breach or end violation, or (2) if cure is not possible, terminate the BA Agreement, and (3) if neither cure nor termination is possible, report breach to Secretary of HHS.
  - But, will regulations/guidance further expand BA’s Privacy Rule obligations?

Expanded Requirements for BAs

- Changes to business associate contracts
  - ARRA provides that security and privacy changes “shall be incorporated into the business associate agreement between the business associate and covered entity”
  - For new contracts entered into after Feb. 17, 2010, CEs advised to make sure provisions are included to ensure compliance by BAs
  - Not clear whether existing contracts need to be amended or whether new provisions incorporated as a matter of law
    - While doubtful that changes would be considered automatically incorporated, guidance on this from HHS would be welcome
Expanded Requirements for BAs

- Changes to business associate contracts
  - CEs (including GHPs) should review their BA contracts and be prepared to make needed modifications
    - Until further guidance is issued, however, most entities will likely take a “wait and see” approach on modifying BA contracts
  - BAs (TPAs and other service providers) should take a proactive approach to identifying their status as a BA and entering into BA contracts with CEs, when required
    - Review existing safeguards and policies and procedures to determine what gaps exist relative to enhanced obligations
      - Some BAs may be more prepared than others but all need to have formal compliance program going forward
      - Note: Requirements would seem to apply even if BA and CE fail to execute a written BA contract (perhaps, unknowingly)

Notification of Breach Requirements

- **Pre-ARRA Rule**: No affirmative obligation to notify individuals or HHS of a breach of Privacy or Security Rules. Rather, CEs’ obligation to mitigate any harm caused by a breach may have included notification of breach.
Notification of Breach Requirements

- **Under ARRA**, if security of “Unsecured PHI” is “breached,” CE must provide notice without unreasonable delay and within 60 days after “discovery” of breach:
  - **To the Impacted Individual**: Individual written notice sent to last known address (with special rules if imminent misuse is possible or individual’s address is unknown).
  - **To the Media**: If breach involves more than 500 individuals in state or jurisdiction, notice through major media outlets.
  - **TO HHS**:
    - If breach involves more than 500 individuals, CE notifies HHS immediately, and HHS will identify CE on its website.
    - If breach involves less than 500 impacted individuals, CE logs the breach and provides the log to HHS on an annual basis.
  - If BA discovers breach, notifies CE.

Breach Rules

- In order for breach to occur, four requirements
  - Unsecure PHI (written, electronic, or spoken)
  - Used or disclosed in an unauthorized manner
    - Including disclosure in excess of minimum necessary
  - “Significant risk of financial, reputational, or other harm”
    - Look at to whom info disclosed, type of info, steps taken upon discovery
  - Use/disclosure does not fall under an exception
    - Unintentional access by employee of BA or CE
    - Inadvertent disclosure between similarly situated employees
    - Recipient could not reasonably retain information
Notification of Breach Requirements – “Unsecured PHI”

- “Unsecured PHI” is PHI not secured through use of a technology or methodology identified by HHS as rendering the information unusable, unreadable or indecipherable to unauthorized persons.
  - On April 17, 2009, HHS issued its initial guidance related to the acceptable technologies and methodologies, which identifies two acceptable methods for securing PHI:
    - Encryption (electronic)
    - Destruction (electronic and paper)
  - HHS-identified technologies and methodologies are intended to be exhaustive, not illustrative.
  - Use of the HHS-identified technologies and methodologies is not required, but such use acts as a “safe harbor.”
  - HHS intends to issue additional guidance on this topic, and is seeking comments by May 21, 2009 on a variety of related topics.
- Notification Requirements only triggered by breach of “unsecured PHI.”

Notification of Breach Requirements – “Discovery”

- A breach is “discovered” as of the first day that it is known (or reasonably should have been known) to the CE or BA.
- The CE or BA has knowledge of the breach on the day that any employee, officer or other agent has such knowledge (except for the individual who committed the breach).
Notification of Breach Requirements – Content and Effective Date

- **Notice Content:**
  - Brief description of breach, including dates;
  - Description of types of unsecured PHI involved;
  - Steps impacted individual should take to protect against potential harm;
  - Brief description of steps CE has taken to investigate incident, mitigate harm and protect against further breaches; and
  - Contact information.

- **Effective Date:** HHS issued interim final regulations August 24, 2009. Notice Requirements will apply to breaches discovered on or after 30 days following date regulations issue (September 23, 2009).

Breach Notification

- **Plan Action Required**
  - Establish Notice Procedures
    - Will CE handles notice or BA?
  - Maintain a breach log
    - Required to be filed with HHS with 60 days of year end
  - Update/modify BAAs to address breach obligations
  - Implement breach training
  - Address breach requirements in policies and procedures manual
Minimum Necessary Standard

- Generally, uses, disclosures and requests by a CE are limited to the information that is the **minimum necessary** to accomplish the intended purpose.
- Pre-ARRA, “minimum necessary” was an undefined, flexible standard.
- By August 2010, HHS will issue guidance on what constitutes “minimum necessary.”
- Starting February 17, 2010 and until guidance issues, CE may only use, disclose, or request **limited data set** information, or if more information is needed, in compliance with the minimum necessary standard.

Prohibition on Sale of PHI

- CE or BA cannot receive remuneration, directly or indirectly, for any PHI unless per a valid authorization specifically addressing sale.
- **Exceptions:**
  - For public health activities;
  - For research (cost of data prep and transmittal);
  - For treatment;
  - For Health Care Operations (HCO) related to sale or transfer;
  - For payment of BA for services under BAA;
  - To provide an individual with his/her PHI; and
  - For other instances permitted by the Secretary in further guidance.
- **Effective Date:** Regulations to issue by August 2010. Effective six months thereafter.
Marketing & Health Care Operations

A communication by CE or BA that is about a product/service and encourages recipient to purchase or use same is NOT considered an HCO.

UNLESS it:
- describes a health-related product/service (or payment for same) that is provided by or included in the plan of CE making communication;
- is for treatment; or
- is for case management or care coordination for the individual or to direct/recommend certain alternative treatments, therapies, health care providers, or settings of care to the individual.

Marketing & Health Care Operations (con’t)

However, if a communication meets one of the exceptions in prior slide and CE receives payment, directly or indirectly, for making such communication, then it is NOT an HCO

EXCEPT where:
- The communication describes only a drug/biologic currently prescribed for recipient and any payment received by CE for making communication is “reasonable in amount”; AND
  - CE makes communication and CE obtains authorization from recipient; OR
  - BA makes communication on behalf of CE and communication is consistent with BA Agreement.
Personal Health Records (PHR) Vendors

- PHRs are e-records that contain an individual’s health information (possibly from multiple sources), and are managed, shared and controlled by or for an individual.
- PHR Vendors are not CEs (but are BAs if they contract with CEs).
- Now, ARRA requires PHR Vendors to notify individuals and the FTC if “Unsecured PHR identifiable health information” is breached.
- Effective Date: Interim final regulations issued by FTC on August 25, 2009 (and FTC issued proposed Health Breach Notification Rule on April 16). Effective 30 days after interim final regulations are issued.

Increased Enforcement Mechanisms

- **Increased Audits.** HHS will conduct periodic audits of CEs and BAs, even if no complaint filed.
- **“Willful Neglect:”**
  - Audit *required* if preliminary investigation of complaint indicates “willful neglect.”
  - HHS is *required* to impose a penalty for violations due to willful neglect.
- **Effective Date:** February 2011. Regulations to issue by August 2010.
Increased Enforcement Mechanisms (con’t)

- **State AGs.** State AGs are authorized to bring a civil action for HIPAA violations to enjoin violations and seek damages on behalf of residents.
  - Damages calculated by multiplying number of violations by $100. Not to exceed $25,000 for all violations of an identical requirement during a calendar year.
  - Court may award costs and reasonable attorneys’ fees to State.
  - State action may NOT be brought during pendency of Federal action.
  - **Effective Date:** Immediately.

Increased Enforcement Mechanisms (con’t)

- **Individual Compensation.** Mechanism for individuals to recover portion of HHS civil penalty or monetary settlements.
  - **Effective Date:** Regulations to issue by February 2010. Effective on or after date of regulations.

- **Annual Reports to Congress.** HHS is required to report to Congressional Committees regarding complaints filed and the disposition thereof, which will be available to the public.
Increased Tiered Penalties

- **Increased Tiered Penalties:**
  - **Tier 1:** If person is not aware of the violation (and would not have known with reasonable diligence), penalty is at least $100/violation, not to exceed $25,000 for all violations of the same requirement in the same calendar year.
  - **Tier 2:** If violation is due to “reasonable cause” (but not willful neglect), penalty is at least $1,000/violation, not to exceed $100,000 for all violations of the same requirement in the same calendar year.
  - **Tier 3:** If violation is due to willful neglect and is corrected in 30 days, penalty is at least $10,000/violation, not to exceed $250,000 for all violations of the same requirement in the same calendar year.
  - **Tier 4:** If violation is due to willful neglect and is not corrected in 30 days, penalty is at least $50,000/violation, not to exceed $1.5 million for all violations of the same requirement in the same calendar year.
- **Effective Date:** Increased penalty amounts apply immediately. “Willful neglect” provisions not applicable until February 2011.

**HIPAA/HITECH Action Items**

- Review Privacy and Security Policies and Procedures to ensure ARRA provisions are incorporated and implemented as they become effective.
  - How are Breach Notification requirements addressed?
- Review Privacy Notice to determine whether any revisions are necessary.
- Review and revise BAAs to incorporate expanded obligations under ARRA’s Amendments to HIPAA as they become effective.
- Provide training to employees with access to PHI regarding ARRA’s Amendments to HIPAA.
- “Audit” practices for compliance with HIPAA and ARRA’s Amendments to HIPAA.
- Business Associates should adopt and implement, at a minimum, HIPAA Privacy and Security Policies and Procedures to reflect their new obligations under ARRA.