

Morgan Lewis

# ARRA's Amendments to HIPAA Privacy & Security Rules

Georgina L. O'Hara  
Jessica R. Bernanke

April 29, 2009

[www.morganlewis.com](http://www.morganlewis.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.

# Overview of Amendments to HIPAA Privacy and Security Rules

- Expanded Obligations of Business Associates (BAs)
- Affirmative Notification of Breach Requirements
- Guidance on “Minimum Necessary” Standard
- Prohibition on Sale of PHI
- Restrictions on Marketing
- Limited Application to Personal Health Records (PHR) Vendors
- Increased Enforcement and Penalties, including application to BAs
  
- Note: This presentation relates to obligations of employer-sponsored health plans, not health care providers or healthcare industry companies 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 Obligations of BAs (con't)

- 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 BAs' Privacy Rule obligations?

# 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.

# 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 – “Breach”

- “**Breach**” generally is the unauthorized acquisition, access, use or disclosure of PHI that compromises the Privacy or Security of that information, excluding certain unintentional or inadvertent disclosures.

# Notification of Breach Requirements – “Discovery”

- A breached 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 is directed to issue interim final regulations no later than August 16, 2009. Notice Requirements will apply to breaches discovered on or after 30 days following date regulations issue.

# 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 due from FTC on August 16, 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 2012. 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 Action Items

- Review Privacy and Security Policies and Procedures to ensure ARRA provisions are incorporated and implemented as they become effective.
- 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.

# Questions?

# Contact Information

- Jessica Bernanke
  - 202.739.5447; [jbernanke@morganlewis.com](mailto:jbernanke@morganlewis.com)
- Georgina O'Hara
  - 215.963.5188; [go'hara@morganlewis.com](mailto:go'hara@morganlewis.com)

# Disclaimer

This communication is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship.