

HIPAA Changes in HITECH

Alabama HIMSS Conference
October 1-2, 2009

Source of Changes to HIPAA

- American Recovery and Reinvestment Act of 2009 (commonly referred to as the “Stimulus Bill”) was signed into law on February 17, 2009.
- Health Information Technology for Economic and Clinical Health Act or HITECH Act is a section within ARRA and addresses a variety of healthcare and technology issues
- Subtitle D within HITECH deals with HIPAA changes

Significant Changes in Subtitle D of HITECH

- Changes to Enforcement Penalties and Mechanisms—increased audits
- Business Associate HIPAA Applicability
- Data Breach Notification
- Accounting of Disclosures/Accounting of Restrictions
- Prohibition on Sale

Enforcement Changes—State Attorney General

- A state Attorney General can now bring an enforcement action in federal court on behalf of state residents to stop violations and obtain damages
- State must serve prior notice on HHS
- HHS may intervene in the state action
- The state can't bring an action if there is an ongoing action from HHS
- Effective now

Increase in Civil Monetary Penalties

- \$100 - \$50,000 for each violation depending on the violation category
- Total penalty can't exceed \$1.5 million in a single calendar year for multiple violation of a single requirement
- Effective February 18, 2009

Categories of Violations

- Low: “did not know (and by exercising reasonable diligence would not have known)”
- Medium: “violation due to reasonable cause and not willful neglect”
- High: “violation due to willful neglect” (as of 2/2011, must impose CAP if found)
- Highest: “violation due to willful neglect” and violation is not corrected

Civil Monetary Penalty Distribution

- Effective February 2010, CMPs collected from violations of Privacy or Security Rule shall be transferred to OCR to enforce the provisions of the Privacy and Security Rules
- In August 2010, the GAO will issue a report on the distribution of collections to individuals harmed by the violations
- By February 2011, HHS has to issue regulations on the distribution of collections to individuals harmed by the violations

Impact of Enforcement Changes

- HHS has more resource to investigate
- State Attorney Generals can investigate
- Individuals may ultimately have a path to receiving compensation for harm from the process of HHS fines
- The cost of Civil Monetary Penalties has the potential to be significantly higher

Changes for Business Associates

- Security Rule requirements for administrative, technical and physical safeguards extend directly to Business Associates
- BA uses of PHI have to be in accordance with the Privacy Rule
- New requirements of the HITECH Act extend to BA's and must be included in Business Associate Agreements
- Civil and Criminal Penalties apply to Business Associates
- Sec. 13408: includes HIE, RHIO, e-prescribing gateway

Implementation Decisions

- Do we need to re-do all Business Associate Agreements? Are there other ways to put our BA's on notice?
- Is it too costly to be a Business Associate for a Covered Entity?
- The impact that additional guidance may have when issued in February 2010

Data Breach Notification—General Rule

Notification in the Case of Breach: *“A Covered Entity that accesses maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses **unsecured protected health information**...shall in the case of a **breach** of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been accessed, acquired, or disclosed as a result of the breach.”*

Data Breach Notification—Business Associate

Notification of Covered Entity by Business Associate: “A *business associate of a covered entity that accesses maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses **unsecured protected health information** shall, following the discovery of a **breach** of such information, notify the covered entity of such a breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, or disclosed during such breach.*”

Data Breach Notification--Key Dates

- Feb 17, 2009: Bill passes
- April 17, 2009: Guidance issued
- August 24, 2009: Interim Final Rule
- September 23, 2009: Data Breach notification rule in effect
- Feb 22, 2010: Grace period ends and penalties apply to non-compliance

Definition of a Breach

- Must be unauthorized access, use or disclosure of PHI which violates Privacy Rule
- Must pose a significant risk of financial, reputational, or other harm to the individual
- Breach does not occur if PHI is part of limited data set and does not include zip codes or DOB

Determining Risk of Financial, Reputational or other Harm

- To whom was PHI disclosed (another CE?)
- Steps taken to mitigate harm
- Is PHI returned prior to use? (can't delay notice)
- If nature of PHI is minimal (name + ID but no health service information)

Exceptions to Breach

1. Unintentional acquisition, access, or use of PHI by a workforce member....if such....was made in good faith and within the scope of authority and does not result in further use or disclosure
2. Inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA
3. Disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably retain the information

Data Breach Notification—Unsecured Protected Health Information

- Two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals:
 - Encryption
 - Destruction

Encryption & Destruction Standards

- Electronic PHI has been encrypted
 - Data at Rest: NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.
 - Data in Motion: Federal Information Processing Standards (FIPS) 140-2. These include standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated
- The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
 - Paper, film, or other hard copy media have been shredded or destroyed
 - Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*

Planning to Minimize Risk

- Group that can respond & manage risk assessments
- Best preventive measure is to encrypt
- Pre-planned steps for media and communications
- Arrangements with Business Associates on how to give notice—don't wait until an incident happens
- Burden of Proof of compliance on CE/BA

Data Breach Notification

● Timing

- Notice must be sent to individuals not later than 60 days after the date of discovery
- “Discovery” is the first day on which a covered entity or business associate employee, officer, or other agent (other than the person committing the breach) knows or should have reasonably known that a breach occurred
- Law Enforcement delay

Data Breach Notification

- Method of Notice to Individuals
 - First class mail to the individual unless agreed to electronic notice
 - If there is insufficient or outdated information, substitute notice must be given
 - If under 10 individuals, substitute notice may be given by phone. If 10 or more individuals given substitute notice, it must be more conspicuous such as posting on the organization website, broadcast media or print media in the geographic areas where the affected individuals are likely to live. Substitute notice must also include a toll-free number for individuals to call for further information.
 - NOTE: If the nature of the breach puts the individual in imminent danger of misuse of unsecured PHI, the covered entity may also notify via telephone.

Content of Notice to Individual

- Brief description of breach
- Type of information disclosed
- Any steps individual should take
- Steps taken to investigate and mitigate
- Contact procedures
- No sensitive information should be included

Data Breach Notification

- Media Notice
 - Required if the breach affects 500 or more persons of a state or jurisdiction.
- Notice to HHS Secretary
 - Immediate notice required and HHS will post to their website if the breach affects 500 persons or more
 - Must be logged and log sent annually to HHS if breach affects less than 500 persons
- Law Enforcement Exception

Data Breach and Business Associates

- Notice not required to specific CE official
- Discovery date imputed to CE if acting as an agent
- Discovery data not imputed if acting as an individual contractor
- BA should not delay notice to CE to gather all info—and should give additional info to CE even after 60 days
- CE/BA work out who sends the notice to individuals

Data Breach and State Law

- HIPAA generally pre-empts state data breach notification law
- State law contrary only if “a CE could find it impossible to comply with both” or if stands as an obstacle to objective
- Example of state law requiring notice within 5 days of data breach
- Additional data elements required by State do not create conflict

PHR's and Data Breach Notification

- Vendors of Personal Health Records and PHR-related entities must notify their customers of any breach of unsecured, individually identifiable health information
- These include vendors of online applications that interact with PHR's
- HHS to study with FTC privacy, security and breach notification requirements (1 year)

PHR's and Data Breach Notification

- Under the FTC Rule, “breach of security” is defined as the acquisition of unsecured PHI of an individual in a PHR without the authorization of the individual
- Breach of security presumed when there is unauthorized access to the data
- Encryption and Destruction can show that PHI is secure

PHR's and Data Breach Notification

- Individuals must be notified within 60 days of the date of discovery
- FTC must be notified in 10 days
- If the breach affects 500 or more people, the media must be notified
- When a vendor provides PHR under a BAA and independently to consumers and the breach affects both parties, the vendor can issue the same notice to all

Restrictions on Certain Disclosures

- Individual can restrict disclosure of PHI if the disclosure is to a health plan for carrying out payment or operations and patient has paid in full
- A CE or BA can't receive payment in exchange for PHI of an individual unless the CE has an authorization.

Exceptions

- Public Health Activities
 - Research
 - Treatment
 - Health Care Operations
 - Remuneration from CE to BA
 - Individual with copy of individual's PHI
 - As determined by the Secretary
- Effective anticipated 2/2011

Accounting of Disclosures

- Treatment, Payment and Operations have been exempted previously when persons requested an accounting of disclosures
- There is no longer an exception for excluding TPO in an accounting of disclosures
- A request for an accounting of disclosures can be for up to 3 years of disclosures from the day on which the accounting is requested

Accounting of Disclosures

- What is a disclosure?
 - Release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information
 - There are still a list of exceptions in 164.528 from the accounting of disclosures including national security, law enforcement, pursuant to an authorization, etc.

Accounting of Disclosures

- Upcoming Clarification
 - Regulations on what information shall be collected about each disclosure from HHS not later the 6 months after the date on which the Secretary adopts standards on accounting for the disclosures.

Accounting of Disclosures

- Business Associates
 - BA's still have to give an accounting of disclosures
 - Covered entities have two ways this can be done
 - Providing the accounting itself for all disclosures by the covered entity and by the business associate
 - Provide the accounting itself for all disclosures by the covered entity and “provide a list of all business associates acting on behalf of the covered entity, including contact information for such associates” (such as mailing address, phone and email address)

Accounting of Disclosures

- Effective Dates
 - For electronic health records in existence as of January 1, 2009, the implementation date is January 1, 2014
 - For electronic health records in existence later than January 1, 2009, the implementation date is January 1, 2011
 - The Secretary reserves the right to change these implementation dates but the dates can't be changed to any later than 2013 and 2016.

Questions?

Richard Chapman

richard@informationinventory.com

502.316.0828