



The HITECH Act: Recent Changes to HIPAA Privacy and Security Rules

Jennifer Landrum Elliott
Stites & Harbison PLLC

jlelliott@stites.com

502.681.0682

“HITECH” Health Information Technology for Economic and Clinical Health Act of 2009

- Section of American Recovery and Reinvestment Act (ARRA) enacted on February 17, 2009
- Creates incentives to use electronic health records; promotes electronic use and exchange of health information
 - Congress linked incentives to “improved” privacy and security rules
 - Act has little to do with electronic health records
- Biggest change to health care privacy and security since the original HIPAA Privacy Rule in 2000
- Focus on
 - changes to HIPAA Privacy and Security Rules
 - Increased enforcement
 - Increased accountability for “Business Associates”

HIPAA Overview

Health Insurance Portability and Accountability Act of 1996

■ *Who*

- Covered Entities: health plans, health care clearinghouses, health care providers
- Business Associates: work with covered entities, receive patient health records
 - Accounting firms
 - Law firms
 - Software vendors
 - TPAs of self-insured health plans
 - Transcriptionists
 - Interpreters
 - Collection agencies

■ *What*

- Protected Health Information (“PHI”)
 - relates to an individual’s health, health care treatment, or health care payment;
 - is transmitted or maintained in any form (electronically, paper, or oral); and
 - can reasonably be used to identify an individual
- e.g. Medical Records, EOBs, Actuarial reports



Security Rule vs. Privacy Rule

- Privacy Rule:

- Applies to PHI in all forms -- electronic, written, and oral

- Security Rule:

- Only applies to PHI created, received, maintained, or transmitted in *electronic* form



HITECH's Impact on HIPAA

1. Increase in Enforcement
2. Extends HIPAA obligations to Business Associates
3. Breach Notification Rule



HITECH's Impact on HIPAA:

Increase in Enforcement

- Civil monetary penalties range from \$100 to \$50,000 per violation, with annual caps ranging from \$25,000 to \$1,500,000 for violations of the same requirement
- Criminal penalties vary from \$50,000 and/or 1 year imprisonment to \$250,000 and/or 10 years

HITECH's Impact on HIPAA: Increase in Enforcement

- HHS to conduct mandatory “periodic audits” of CEs and BAs to ensure compliance with the new provisions
 - Approximately \$10 Billion has been appropriated to fund audits
- State Attorneys General - action in U.S. District Court on behalf of residents of the state who have been threatened or adversely affected by a HIPAA violation
 - May collect fines/penalties as damages, as well as costs and attorneys fees
- “Whistleblowers” coming soon – GAO recommendations on apportioning CMPs to those harmed by violations due Aug. 2010
 - HHS must adopt methodology by Feb. 2012
 - Increases incentives for individuals to file complaints
- New “Breach Notification” rules establish affirmative reporting duties and *make penalties easier to assess*

Enforcement Examples: Pre-HITECH

- Providence Health & Services – July 16, 2008
 - Backup tapes, optical disks, and laptops removed from office and subsequently lost or stolen
 - 386,000 Individuals impacted
 - Required to revise policies and procedures for physical and technical safeguards – e.g. staff training, encryption, policies for off-site transport, and storage of electronic media
- \$100,000 penalty and Corrective Action Plan

Enforcement Examples: Pre-HITECH

- CVS Pharmacy – January 16, 2009
 - Disposed of prescription bottles in publicly accessible dumpsters without removing labels
 - “millions of health care consumers” impacted
 - Failed to implement adequate safeguards to secure PHI; failed to train employees on proper disposal of information, failed to maintain sanctions for workforce members who failed to comply with policies
- \$2.25 million and Corrective Action Plan

HITECH's Impact on HIPAA: Business Associates

Pre-HITECH

- Indirectly required to comply with HIPAA Privacy Rule by virtue of BAAs
- Consequence: *breach of contract; indemnify clients for fines/claims against them; loss of client*
 - Not directly subject to HHS fines and penalties

HITECH's Impact on HIPAA: Business Associates

Security Rule

- **Effective Date: Feb. 17, 2010**
- BAs are now directly subject to the “administrative, physical, and technical safeguard requirements” of the HIPAA Security Rule
- Still required to comply with Business Associate Agreements
- Also required to maintain policies, procedures, and documentation of security activities “in the same manner that such sections apply to the Covered Entity.”



HITECH's Impact on HIPAA: Business Associates

New Security Rule Obligations:

1. Implement written policies and procedures that address each Security Rule administrative, technical, and physical safeguards.
2. Implement security awareness and training.
3. Designate a security official.
4. Conduct an “accurate and thorough” security risk analysis

HITECH's Impact on HIPAA: Business Associates

Privacy Rule

- **Effective Date: Feb. 17, 2010**
- BAs are now statutorily required to only use or disclose PHI consistent with its obligations under its BAAs.
- Not obligated to implement the full range of HIPAA Privacy requirements (e.g. Notice of Privacy Practices, etc.)
- What if there is no existing BAA b/w parties because of oversight? Is obligation to enter into a BAA now also a responsibility of BA?



HITECH's Impact on HIPAA: Business Associates

Applicability of Penalties

- Business Associates that violate an applicable HIPAA provision or who violate a term of a Business Associate Agreement will be subject to the same civil and criminal penalties as Covered Entities.



HITECH's Impact on HIPAA: Breach Notification Rule

- Affirmative duty to notify individuals and report certain HIPAA violations to HHS under “Breach Notification” rules
- Covered Entities and Business Associates must comply
- Effective 9/23/09; Enforcement 2/22/10

HITECH's Impact on HIPAA: Breach Notification Rule

- *Incident must be a HIPAA Violation*
unauthorized use, access, disclosure of PHI
- *That “poses a significant risk of financial, reputational, or other harm to the individual”*
- *The PHI involved must be “unsecured”*
“not rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology/methodology specified by HHS” (*in other words, not encrypted*)
- *Not subject to an exception*

HITECH's Impact on HIPAA:

Breach Notification Rule

- Individual whose PHI was subject of breach when, what, efforts to investigate, steps to mitigate, contact for additional information
- HHS
 - *immediately* if 500+ individuals;
 - Log and report *annually* for breaches under 500 people
- Prominent Media Outlets if breach involves 500 individuals who are residents of one state or jurisdiction



So What Should You Do?

■ Considerations for Audit Plan:

- Has your organization entered into new/amended BAAs to incorporate HITECH provisions?
- Are you effectively capturing information about privacy and security breaches from employees and others?



So What Should You Do?

■ Considerations for Audit Plan:

- Are you notifying individuals, HHS and/or media about breaches in accordance with HITECH?
- Are your BAs notifying you about breaches?
- If your organization is a Business Associate, have you developed a Security Policy and taken necessary steps to comply with the Security Rule? Are you tracking responsibilities under your BAAs?