



United States Department of
Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HIPAA Privacy and Security Rules in a HITECH World

August 20, 2009

Susan McAndrew, J.D.
Deputy Director,
Health Information Privacy



American Recovery and Reinvestment Act of 2009

- Title 13: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Subtitle A: Promotion of HIT through the Office of the National Coordinator for HIT (ONC)

Subtitle B: Testing of HIT through the National Institute of Standards and Technology (NIST)

Subtitle C: Grants and Loan Funding for Incentives for the Use of HIT

Subtitle D: Privacy (Privacy Rule and Security Rule)



Why HITECH Matters

- HITECH creates significant incentives for an expanded use of electronic health records
- EHRs, PHRs, HIEs (electronic exchanges) expected to be transformational for both cost and quality
- HIPAA Privacy and Security embedded as applicable law to protect consumer interests



Breach Notification

- Covered entities must notify each affected individual of breach of “unsecured protected health information.”
- Business associate must notify covered entity of breach
- Notice to media if more than 500 people affected.
- Notifications to be provided without unreasonable delay (but no later than within 60 days) of discovery of breach.
- Notice to Secretary of breach and posting on HHS Website.
- FTC to regulate similar notice requirements similar for PHR vendors not subject to HIPAA
180 days for IFR
- HHS and FTC to study oversight and make recommendations to Congress (02/2010)

Interim Final Regulations required
within 180 days after enactment.



Breach Notification Deliverables to Date

- HHS Breach Notification Guidance and Request For Information :
 - Guidance on the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Request for comments with respect to the guidance and to inform interim regulations pertaining to breach notification –May 21, 2009.
- FTC Notice of Proposed Rulemaking and Request for Public Comment :
 - Rules requiring vendors of PHRs and related entities to notify individuals when the security of their individually identifiable health information is breached. Request for comments with respect to proposed rules –June 1, 2009.



Business Associates

- Applies the HIPAA Security Rule's requirements for administrative, physical, and technical safeguards, policies and procedures, and documentation directly to business associates.
- Provides that a business associate may use or disclose PHI only if such use or disclosure is in accordance with the HIPAA Privacy Rule's required terms for business associate contracts.
- Any entity that provides data transmission of PHI to a covered entity and that requires routine access to PHI (such as Health Information Exchange Organization) or that contracts with a covered entity to provide a PHR is a business associate and must have a business associate agreement with the covered entity.
- Extends HIPAA's civil and criminal penalties to business associates for violations of these provisions.

Effective Date: 2/2010



Accounting & Access for EHRs

- If covered entity maintains an electronic health record (EHR), covered entity must include in an accounting disclosures through the EHR for treatment, payment, and health care operations for the three years prior to the request.

Effective Date: Depends on CE's adoption of EHR

- If covered entity uses an EHR, individual has a right to a copy of his PHI in electronic format.

Effective Date: 2/2010



Other HIPAA Privacy Changes

- **Right to Restriction:** Covered entity must comply with individual's request for restriction if disclosure: (1) is to health plan for payment or health care operations and (2) pertains to item/service for which provider was paid in full "out-of-pocket."
- **Marketing:** Places additional restrictions on covered entity making certain communications about products or services, where entity receives payment in exchange for communication.
- **Fundraising:** Covered entity's fundraising communications must provide clear opportunity for individual to opt out of future communications. **Effective 2/2010**



Other HIPAA Privacy Changes

- **Minimum Necessary:** Covered entity must limit PHI, to extent practicable, to limited data set, or, if necessary, to minimum necessary. HHS to issue guidance on what constitutes minimum necessary. **Effective 2/2010 but sunsets after guidance is issued**
- **Sale of PHI:** No direct or indirect remuneration in exchange for PHI, unless the individual signed an authorization; exceptions for public health, research, treatment, sale of business, business associate activities, individual access, and others as determined by Secretary. **Effective Date: Regulations required within 18 months after enactment; provisions apply 6 months later.**



Improved Enforcement

HITECH Act:

- Noncompliance Due to Willful Neglect
- Distribution of Certain Civil Monetary Penalties
 - Transfer to OCR for Enforcement
 - Percentages to Harmed Individuals
- State Attorneys General
- Periodic Audits
- Criminal Penalties for Individuals (Employees)

Other: Secretary's Delegation of Security Rule Enforcement to OCR – July 27, 2009



CMP Categories

- If “person did not know” or “by exercising reasonable diligence would not have known.”
- If the violation was “due to reasonable cause and not to willful neglect.”
- If the violation is due to willful neglect, and is corrected during 30-day time period.
- If the violation is due to willful neglect, and is not corrected during 30-day time period.

Effective Date: Violations
occurring after 2/18/2009



Increase in CMPs

- CMPs for Violations Occurring Before the HITECH Act (before February 18, 2009)
 - Up to \$100 per violation;
 - Capped at \$25,000/calendar year for multiple violations of an identical requirement or prohibition.
- CMPs for Violations Occurring After the HITECH Act (on or after February 18, 2009)
 - \$100 to \$50,000 or more per violation;
 - Capped \$1.5 million/calendar year for multiple violations of an identical requirement or prohibition.

Effective Date: Violations
occurring after 2/18/2009



Education on Health Information Privacy

- Regional Privacy Advisors for Education and Guidance to Covered Entities, their Business Associates and Individuals on Privacy and Security of PHI
- Multi-faceted National Education Initiative on Health Information Privacy to Enhance Public Transparency Regarding Uses of PHI, including Programs to Educate Individuals about Potential Uses of Their PHI, the Effects of Such Uses, and their Privacy Rights with Respect to Such Uses



Studies, Reports and Guidance

- Annual Guidance on Most Effective and Appropriate Technical Safeguards to Carry Out the HIPAA Security Rule and the HIT Standards Adopted under HITECH
- Number and Nature of Complaints, Resolutions, Technical Assistance, Audits and Findings and the Secretary's Plan Going Forward
- Application of Health Information Privacy and Security Requirements to Non-HIPAA Covered Entities
- How to Best Implement the Privacy Rule's Requirements for De-Identification
- Definition of "Psychotherapy Notes" and test data that is part of a mental health evaluation



Want More Information?

The OCR website:

<http://www.hhs.gov/ocr/privacy/>

My contact:

Susan.McAndrew@hhs.gov