United States Department of Health & Human Services

Office of the Secretary

Office for Civil Rights (OCR)

Regulations Update HIPAA/HITECH/GINA

NIST/OCR HIPAA Security Assurance Conference

May 10, 2011

Susan McAndrew, J.D.

HHS Office for Civil Rights

OVERVIEW

- Status of Regulatory Activities
  - Genetic Information Non-discrimination Act NPRM (10/01/09)
  - Breach Notifications IFR (08/24/09)
  - Enforcement and Compliance IFR (10/30/09)
  - HITECH Privacy/Security NPRM (7/14/10)
- Coming: Omnibus Final Rulemaking
- Coming: NPRM on Accounting for Disclosures from Electronic Records

HITECH/HIPAA Proposed Rule

- **HITECH Content:**
  - Business associates
  - Enforcement
  - Electronic access
  - Marketing
  - Fundraising
  - No sale of PHI
  - Right to request restrictions
- **Other Content:**
  - Research authorizations, Student immunization records

Business Associates: HITECH

- HITECH Sections 13401 and 13404 make BAs accountable to consumers and to HHS for protecting the privacy and security of protected health information and directly liable for criminal and civil penalties for violations of certain provisions of the HIPAA Privacy and Security Rules.

Business Associates: NPRM

- NPRM proposes:
  - Requiring that BAs comply with the technical, administrative, and physical safeguard requirements under the Security Rule.
  - Prohibiting a BA from making a use or disclosure in violation of the Privacy Rule.
  - Including Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities as BAs.
  - Clarifying that BAs are liable whether or not they have an agreement in place with the CE.
  - Defining subcontractors as BAs; clarifying that BA liability flows to all subcontractors.

Access: HITECH

- HITECH Section 13405(e) strengthens individuals' right to access their protected health information by creating an absolute right to an electronic copy of their health information if the entity maintains the information electronically.

Access: NPRM

- NPRM proposes:
  - Strengthening the right to an electronic copy of PHI in any electronic designated record set, not just in an electronic health record.
  - Permitting a covered entity to charge a reasonable, cost-based fee to cover the labor for copying and electronic media.
  - Giving an individual the right to direct the covered entity to transmit the copy of protected health information directly to another person designated by the individual.

Enforcement IFR

	For violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
PENALTY AMOUNT	Up to $100 per violation	From $100 to $50,000 per violation
CALENDAR YEAR CAP FOR VIOLATIONS OF AN IDENTICAL PROVISION	$25,000	$1,500,000

Enforcement

- NPRM proposes to modify the HIPAA Enforcement Rule regarding:
  - Willful neglect;
  - The definition of reasonable cause;
  - The factors used in determining a civil money penalty amount; and
  - Affirmative defenses.

Proposed Compliance Dates

- Covered entities and business associates will have 180 days from the effective date of the final rule to comply.
- Covered entities and business associates will have up to one year from the compliance date (one year and 240 days from the publication date) to make any necessary changes to existing business associate agreements.
  - Sooner if agreement is renegotiated during this time period.
  - Business associates must still comply with all other applicable requirements of the HIPAA Rules, even if not reflected in agreement.

HIPAA and EHRs: New Opportunities

- Minimum necessary
  - New opportunity to control workforce access
- Patient access and amendment
  - Portals and PHRs
- Improved transparency
  - Audit logs
- Integrity and availability

HIPAA and EHRs: New Challenges

- Updating risk analysis
- Implementing updated risk management plan
- What are the “reasonable and appropriate safeguards”
  - Encryption
  - Access controls
- Integrity and availability

For More Information

- OCR Website: http://www.hhs.gov/ocr/privacy
  - Understanding HIPAA – Special Topics – Health Information Technology
  - Frequently Asked Questions
- My contact:

  susan.mcandrew@hhs.gov