United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

OCR Update

HIPAA Summit West

September 20, 2011

Michael F. Kruley and Michael Leoz

HHS Office for Civil Rights

REGULATORY STATUS

- 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)
- NPRM on Accounting for Disclosures from Electronic Records (5/31/11)
- Coming: Omnibus Final Rulemaking

HITECH/HIPAA Proposed Rule

- **HITECH Content:**
  - Business associates
  - Enforcement
  - Electronic access
  - Marketing
  - Fundraising
  - No sale of PHI
  - Right to request restrictions

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.

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

Breach Notification
45 CFR 164 Subpart D

- HHS Issued RFI & Guidance – April 2009
  - Guidance on Technologies/Methodologies for unusable, unreadable, indecipherable PHI
  - 74 Federal Register 19006 (April 27, 2009)
- HHS Issued IFR – August 2009
  - Effective for breaches after 9/23/09
  - 74 Federal Register 42740 (August 24, 2009)

Breach Notification IFR

- Covered entities and business associates must provide notification of breaches of ***unsecured*** protected health information

- HHS Breach Notification Guidance: PHI is "unsecured" if it is NOT
  - Encrypted
  - Destroyed

What is a Breach

- Impermissible use/disclosure which "compromises privacy/security" of PHI
  - Poses a significant risk of harm
    - Financial
    - Reputational
    - Other harm
- Determined through risk assessment

Exceptions for Harmless Error

- Exceptions for inadvertent, harmless mistakes
  - Unintentional access by workforce member and no further impermissible use or disclosure
  - Inadvertent disclosure at same CE/BA/OHCA and no further impermissible use or disclosure
  - Recipient could not reasonably have retained the PHI

Breach Notification Requirements

Covered entity must:

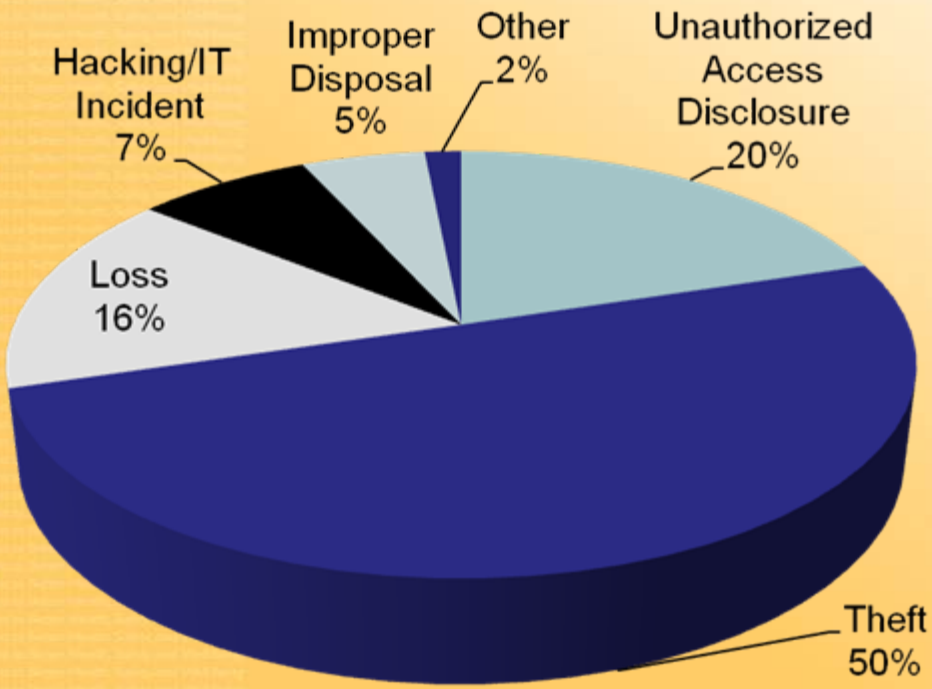
- Notify each affected individual of breach
- Notify Secretary via OCR's website
- Notify media if more than 500 people affected in state/jurisdiction

Without unreasonable delay after discovery of breach – can report "small" breaches annually

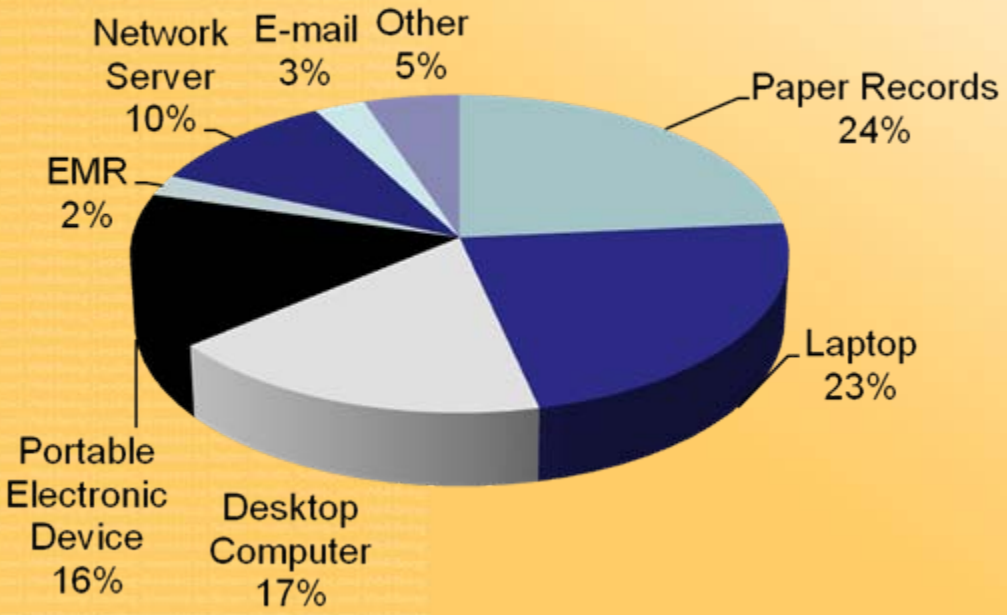
OCR Breach Investigations

- OCR opens a review of all breach reports involving >500
- CE should be prepared to respond with:
  - Determination of the root cause of disclosure
  - Identifying gaps in compliance with Privacy and Security Rules that led to the breach
  - Provide evidence that the root cause has been addressed to insure that further breaches do not occur

Breach Notification:
500+ Breaches by Type of Breach



Breach Notification:
500+ Breaches by Location of Breach



Breach Notification Statistics
(as of August 12, 2011)

- 300 reports involving over 500 individuals
- Over 34,000 reports involving under 500 individuals
- Top types of large breaches
  - Theft
  - Unauthorized Access/Disclosure
  - Loss
- Top locations for large breaches
  - Paper records
  - Laptops
  - Desktop Computers
  - Portable Electronic Device

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.

Recent Enforcement Actions

HITECH has allowed the Secretary to impose significantly increased penalty amounts for violations of the HIPAA rules and encouraged prompt corrective action.

Implementation of HITECH Act enforcement has strengthened the HIPAA protections and rights related to an individual's health information.

This strengthened penalty scheme will encourage covered entities and business associates to comply with the HIPAA Privacy and Security and HITECH requirements.

Cignet Health Care

- Cignet Health Care is a treatment provider and health plan issuer
- Over a two-year period, 41 individuals complained to OCR that Cignet had ignored their requests for access to their health records
- Cignet failed to respond to OCR's investigation or provide copies of the patients' records

CMP of $4.3 Million Levied

- Civil Money Penalty of $1.3 million attributable to failure to provide individuals access to their health records

- Penalty of $3 million for failure to respond to OCR demands to produce records and failure to cooperate with OCR's investigation

Massachusetts General Hospital

- Large multi-specialty healthcare provider
- Employee, who had taken patient files home, left the folders on the subway train and they were never recovered
- Investigation initiated after media reports of incident and a complaint from an individual whose PHI was lost
- Settled with OCR through Resolution Agreement and Corrective Action Plan

Actions to Settle Case

- $1 million resolution amount
- Corrective Action Plan
- MGH required to actively monitor its compliance with the Corrective Action Plan through use of an internal monitor

Rite Aid Corporation

- Large US pharmacy chain
- Series of media reports about personnel disposing of PHI, including labeled pill bottles and prescriptions, in unsecured garbage containers outside of several Rite Aid pharmacy stores
- Settled with OCR through Resolution Agreement and Corrective Action Plan
- Simultaneously settled with FTC through a consent order

Indications of Non-Compliance in Rite Aid Resolution Agreement

- Rite Aid policies and procedures for disposal did not reasonably and appropriately safeguard PHI
- Rite Aid did not maintain sanctions policy for workforce members who failed to safeguard PHI in disposal process
- Rite Aid did not provide necessary and appropriate training for its workforce regarding disposal of PHI

Actions to Settle Case

- $1 million resolution amount
- Corrective Action Plan
- Both HHS and FTC require RAC to actively monitor its compliance with the Resolution Agreement and Consent Order

University of California at Los Angeles Health System

- Large multi-campus healthcare provider
- UCLAHS employees repeatedly and without permissible reason looked at the e-PHI of two high profile patients
- From 2005-2008, unauthorized employees repeatedly looked at e-PHI of other UCLAHS patients

Actions to Settle Case

- $865,500 settlement amount
- Corrective Action Plan (CAP)
  - Implement OCR approved Policies and Procedures
  - Training for UCLAHS employees
  - UCLAHS required to actively monitor its compliance with the CAP through use of an independent monitor for 3 years

A Culture of Compliance

- In light of OCR's clearly articulated intention to aggressively enforce the HIPAA Privacy and Security Rules, covered entities and business associates should review their current HIPAA compliance programs.
- A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents.

Audits as Part of OCR Compliance Oversight

- Enforcement
  - Investigation of Complaints
  - Compliance Reviews
- Audit
  - More systematic approach to compliance
  - Preventative (rather than reactive) to close vulnerabilities before they can be exploited
  - Risk-based considerations to selection
  - Increased potential for learning from others

Elements of Audits

- Objective selection criteria for entities
- Standard protocols adapted to entity size/type
- Advance notice
- Preliminary desk review and onsite components
- Report drafting with findings, recommendations
- Reporting on corrective or other actions

Timeline for Audits

- Developmental phase
  - Ongoing over next three months
- Testing phase
  - Through end of January 2012
- Deployment and evaluation
  - Throughout 2012

For More Information

- OCR Website: http://www.hhs.gov/ocr/privacy

Region IX contacts:

Michael Kruley, Regional Manager

Michael Leoz, Deputy Regl. Manager

Main # 415-437-8310

reg9.ocrmail@hhs.gov