U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

**OFFICE FOR
CIVIL RIGHTS**

Health Information Privacy Update

National Committee on Vital and Health Statistics
June 11, 2014
Rachel Seeger, Senior Advisor
HHS Office for Civil Rights (OCR)

Compliance and Enforcement

- 2011-2012 HITECH Reports to Congress Issued
- Investigated Complaints/Compliance Reviews
  - Over 32,600 cases investigated
  - Almost 22,500 closed with correction action
- Resolution Agreements/Corrective Action Plans
  - 21 settlement agreements that include detailed corrective action plans and monetary settlement amounts
  - 1 civil money penalty
- Breach Reports
  - 1,027 reports of breaches affecting 500 or more individuals
  - 116,000 reports of smaller breaches
- Audit Program
  - Phase 1 completed: pilot audits and evaluation
  - Phase 2 in planning stages

Recent Enforcement Highlights

- **NY Presbyterian Hospital and Columbia University - May 7, 2014**
    - Impermissibly disclosed the ePHI of 6,800 patients to Google and other internet search engines
    - Failed to conduct an adequate risk assessment of all IT systems and equipment
    - NYP $3,300,000 monetary settlement and corrective action plan; CU 1,500,000 monetary settlement and corrective action plan

- **QCA - April 22, 2014**
    - Did not implement policies and procedures to prevent, detect, contain, and correct security violations of computer systems containing ePHI
    - Did not implement physical safeguards of all workstations with access to ePHI
    - $250,000 monetary settlement and corrective action plan

- **Concentra - April 22, 2014**
    - Failed to remediate and manage its identified lack of encryption of systems and software containing ePHI
    - $1,725,000 monetary settlement and corrective action plan

- **Skagit County – March 7, 2014**
    - Provided access to ePHI on its public web server
    - No policies and procedures

Some Areas of Concern

- Risk analysis & risk management
- Security and control of portable electronic devices
- Proper disposal
- Physical access controls
- Training
- Lack of senior leadership attention/culture of compliance

Compliance and Enforcement
Audit – What's to Come

Formal Program Evaluation 2013

Internal analysis for follow up and next steps

- Creation of technical assistance based on results
- Determine where entity follow up is appropriate
- Identify leading practices

Revise Protocol to reflect Omnibus Rule

Ongoing program design and focus

- Business Associates
- Accreditation /Certification correlations?

New CMS/OCR Medscape Module
EHRs and HIPAA: Steps for Maintaining Privacy and Security of Patient Information

APRIL - MAY 2014
13.829 learners
47

http://www.medscape.org/sites/advances/patients-rights

More Information

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