Surviving An OCR HIPAA Audit

Wendy Brazil, JD, CHC
Gretchen Keller, RHIA
Neosho Memorial Regional Medical Center
Chanute, KS

Background

- ARRA requires HHS to audit HIPAA compliance.
- OCR initiated a pilot program to perform up to 150 audits of covered entities beginning 11/2011 and concluding 12/2012.
- OCR engaged KPMG to perform the onsite audits using generally accepted government auditing standards

Audit Objectives

- Audits are meant to be a compliance tool rather than an investigation, but may trigger a separate enforcement investigation if serious problems are found.
- Objective is to improve covered entity compliance with HIPAA-will publicize de-identified results, showing weaknesses and best practices.

Notification

- Letter from KPMG LLP
- Off-Site and On-Site Reviews
  - Off-Site
    - Document Request – 15 days
      - General, Privacy, Security
  - On-Site (Fieldwork)
    - 30-120 Days from Date of Letter
    - 3 Auditors
    - 1 Week Duration
    - Draft of Potential Findings – 10 Days to Respond
    - Final Audit Report - 30 days

Document Request - General

- Site Contact Information - who to contact
- Previous Audits, Evaluations or Assessments
- Disclosure of PHI
  - Fundraising or Research
- Audit Survey – Enclosed Attachment
  - Policies – developed in house or parent company
  - Type of Provider
  - Number of Patient Visits
  - Number of Patient Beds
  - Current Number of Clinicians on Staff
  - Current Number of Clinicians with Privileges
  - Use of EMR
  - Total Revenue

Document Request - Privacy

- Privacy Officer Contact Information
- Identify any applicable industry guidance or reference material used to develop any policies and procedures
- Notice of Privacy Practices
- Training documentation for employees over Privacy Practices and Organization Training Policy

Document Request – Privacy

- Policies and Procedures
  - Privacy Policies
  - Administrative, Technical and Physical Safeguards
    - All Forms of PHI
  - Complaint Handling
  - Sanction and Disciplinary over Privacy Violations
  - Mitigation and Disciplinary for Breach

Document Request – Privacy

- Privacy Practices Documentation –
  - Rights to Request Privacy Information
  - Right to Request Privacy Protection
  - Access of Individuals to PHI
  - Denial of Access to PHI Procedures
  - Amendment of PHI
  - Accounting of Disclosures of PHI
  - Administrative Requirements
  - Use and Disclosure

Document Request – Privacy

- Uses and Disclosures
  - Deceased Individuals
  - Confidential Communication
  - Business Associate Contract Requirements
  - Treatment, Payment and/or Operations
  - Consent and Authorization Requirements
  - Judicial or Administrative Proceeding Requirements
  - De-Identified/Re-Identified PHI Procedures
  - Restrictions
  - Identity Verification

Document Request – Security

- Security Officer Contact Information
- Identify any applicable industry guidance or reference material used to develop any policies and procedures
- Risk Assessment
  - Entity Level
  - Systems - House PHI
  - Risk Assessment Procedures
- Organizational Chart

Document Request – Security

- Plans
  - Security Incident Management Plan
  - Disaster Recovery Plan
    - Most Recent Disaster Recovery Exercise Documentation
- List of Role Based Access
  - Job Level and Level of PHI Access
- System Generated User Access Listing
- System Generated Listing of New Hires
  - Past Year

Document Request – Security

- Policies and Procedures
  - Access Control
  - Data Protection
  - Acceptable Use
  - Workstation Security
  - Workforce/HR Security
  - Sanctions

Document Request – Security

- Policies and Procedures Cont.
  - Physical Security
  - Encryption
  - Data Backup and Recovery Procedures
  - Data Destruction and Media Reuse Procedures
  - User Authentication
- HITECH
  - Breach Notification Processes
  - Risk Assessment

On-Site Visit

- Room or Office with Internet Access
- Entrance Conference
  - Slide Presentation
- Walk Through Facility
- Interviews
  - Privacy and Security Officer
  - More Requests….
    - Electronic Format - Email

On-Site Document Request – Privacy

- Screenshots of Admission Screens
  - Notice of Privacy Practice
- Signed Acknowledgement of Notice of Privacy Practices
- Release of Information Form
- Change of Communication Form
- Copy of Training Roster
- Documentation of Breach Assessment

On-Site Document Request – Privacy

- Executed Authorizations
  - Court Order
  - Deceased
  - Request Using NMRMC Form
- Screenshots of Role Based Access
  - Nurse Aide vs Nurse
- Executed Business Associates Agreement
  - HIS Vendor
  - Clearinghouse
  - Other (our pick)

On-Site Document Request – Security

- System Access Form
- Screenshots of Login Screens
- Contingency Plan
- Documentation of Recent Disaster Plan
- Screenshots of Inventory Checks
- Evidence of Destroyed Media/Hardware
- Screenshots of Back-up Confirmation
  - Consecutive Days

On-Site Document Request – Security

- Validation of Encryption
- Screenshot of Clearinghouse Website - https
- VPN Screenshot
  - Hashing Algorithms
  - Encryption
- Screenshot of Audit Logs
  - User
  - Transaction

On-Site Document Request – Security Continued

- Copy of Random Audit Log Audits
- User Access to MS4 Menus
  - Role Base
- Examples and Screenshots on Check-Sum Function

Results

- Top Audit Issues first 20 Audits:
  - Risk Analysis
  - Grant/Modify User Access
  - Incident response
  - Contingency Planning
  - Media reuse and Destruction
  - Encryption
  - User Activity Monitoring
  - Authentication/Integrity
  - Physical Access

More Information

- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Questions ???