KPMG

cutting through complexity

# 2012 HIPAA Privacy and Security OCR Audits

Michael D. Ebert

National HIPAA Services Leader

# Background

- **The American Recovery and Reinvestment Act – HITECH Act §13411(2009):** Requires Health & Human Services (HHS) to provide for periodic audits to ensure that covered entities and business associates comply with HIPAA Privacy and Security Rules and Breach Notification standards.
- **HHS – Office for Civil Rights (OCR) awards two audit contracts (2011)**
  - $180,000 contract with Booz Allen Hamilton
    - Identify audit candidates
    - Provide background and recommendations for audit program
  - $9.2 million contract with KPMG
    - Develop an audit protocol
    - Assess compliance with HIPAA privacy and security regulations
    - Conduct pilot audit program for up to 150 audits of covered entities.
      - Business Associates in subsequent years
      - Identification is based upon Unique Identifiers for Covered Entities

# Regulatory Background - Five Key Areas of Privacy Standards

## Principle Sections of the Privacy Regulations

- General Principles for Uses and Disclosures
- Permitted Uses and Disclosures
- Limiting Uses and Disclosures to the Minimum Necessary
- Notice and Other Individual Rights

- Administrative Requirements
- Organizational Options
- Personal Representatives and Minors
- Breach Notification
- Accounting for Disclosures (DRAFT)

### Boundaries

- Information used only for intended purpose and only as much information as required for the intended purpose
- Consumer use and disclosure statement

### Safeguards

- Administrative, technical, and physical mechanisms to keep information private, confidential and secure within internal operating systems and external communications

### Consumer Control

- Informed consent to use information
- Right to access and amend information
- Authorization for disclosures
- Record of disclosures

### Accountability

- Federal penalties for violations
- Effective compliance activities to deter, identify, and punish violations

### Public Responsibility

- Process for disclosing information for public health, research & legal purposes

# Regulatory Background - Security Rule Standards

## Administrative Procedures

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

## Physical Safeguards

- Facility Access Controls
  - Disaster recovery
  - Emergency Mode
  - Equipment transfers
  - Facility security plan
  - Access Authorization process (physical access)
  - Maintenance records
  - Need to know access
  - Sign in and escort visitors
  - Testing and revision
- Workstation Use
- Workstation Security
- Device and Media controls over hardware and software

## Technical Standards and Mechanisms (Data at rest & data in transit)

- Access and Authorization controls
  - Context based, role based, or user based
  - Encryption
- Audit controls (suspect access attempts)
- Integrity
  - Data authentication
- Personal and Entity Authentication
  - Unique User ID
  - Authentication Technique
    - PIN
    - Token
    - Biometric
    - Call Back
  - Automatic Logoff
- Transmission Controls
  - Access Controls
  - Audit Trail
  - Encryption

# Program Objectives

**The objectives for the audit program are to improve covered entity compliance with the HIPAA privacy and security standards, through two approaches.**

**•OCR anticipates that widely publicizing both the audit program and the results of particular audits will spur covered entities and their business associates to assess and calibrate their privacy and security protections.**

**•In addition, OCR will post on its web site and broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges. Such technical assistance will assist those entities that are seeking information to frame their ongoing compliance efforts.**

**It is the intent of OCR to publish results that were obtained from these reviews as a broader guidance set to the industry (de-identified).**

# Timeline for the Audit Program

**The contract with KPMG to create audit protocols and field the pilot audits went into effect the end of June, so we are now standing up the program activities.  The pilot audit program will be a three step process.**

1. **The first step entails working with KPMG to develop the audit protocols.**
2. **An initial round of audits will be fielded to test the protocols. The results of the field testing will inform final protocol design.**
3. **The last step will include rolling out the full range of audits and an evaluation process. KPMG began field testing the audit protocol in January. All audits will be completed by December, 2012.**

# How will the Audit Program Work

The audit process will include standard components associated with most audits. Audit reports generally describe:

- how the audit was conducted;
- what the findings were and;
- what actions the covered entity is taking in response to those findings.

Entities selected for an audit will be informed of their selection by OCR and asked to provide documentation of their privacy and security compliance. Every audit will include a site visit and result in an audit report.

The final report will incorporate the steps the entity has taken to resolve any compliance issues identified by the audit, as well as describe best practices of the entity.

# What will be the Outcome of an Audit?

Audits are a type of review that serves more as a compliance improvement tool then an investigation of a particular violation that may lead to sanctions and penalties.  An audit may uncover vulnerabilities and weaknesses that can be appropriately addressed through corrective action on the part of the entity.

It is possible that an audit could indicate serious compliance issues that may trigger a separate enforcement investigation by OCR.

# HITECH Act Impact

## HITECH Act (Subcomponent of American Recovery and Reinvestment Act) of 2009

**Though outside of HIPAA title II, this is additional & direct legislation to improve the original HIPAA title II requirements and to define and tighten some open gaps**

- Establishes Breach requirement for Privacy Rule Violation
  - Effective date was September 23, 2009
  - Establishes Scope and Timeline
  - Clarifies definition of Breach
  - Likelihood of harm must be determines/assessed
- Establishes New Penalty Levels
  - Uncorrected willful neglect $1.5 million to Unknowing $25K
- Establishes compliance requirements for all PHI and PHR, whether included in a BA agreement or not.
- Enforcement Broadened to include State A.G.'s and Local Law enforcement

# HITECH Oversight & DHHS Activities

- Enforcement responsibility has been delegated to the Office for Civil (OCR) rights for both Privacy (as of April 13, 2003) and Security (as of July 27, 2009)
- HITECH mandates the creation of a pilot program to assess compliance of Covered Entities with HIPAA.
- Plans by OCR are to conduct up to 150 assessments a year with external service providers and a newly formed examination group.
- States have been additionally involved in privacy exposures and have levied fines in addition to federal guidelines, mostly leveraging State PII laws with HIPAA Title II requirements.
- DHHS's OIG office reviewed 7 hospitals, independent of CMS and OCR for compliance with HIPAA's regulations and found 154 findings with compliance.
- OIG also sighted OCR for lack of enforcement and compliance activities, which led to Congress's mandate in the HITECH Act and OCR's recent Penalty activity.

# Meaningful use: Core set 15 requirements

- Objective:
  - Protect electronic health information created or maintained by the certified eHR technology through the implementation of appropriate technical capabilities.
- Measure:
  - Conduct or review a security risk and implement updates as necessary and correct identified security deficiencies as part of the Eligible Provider’s, Eligible Hospital’s, or Critical Access Hospital’s risk management process per HIPAA Security Rule 45 CFR 164.308(a)(1)
- Perform HIPAA Security Risk Assessment for 3 sets Controls:
  - Application Layer:
  - Infrastructure Layer:
  - Enterprise Controls:
- Evidence of Compliance with Security Rule:
  - Design evidence
  - Operational evidence

# Non-Compliance Risks

- Loss of Contracts
- Criminal and Civil investigation
- Federal and State fines
- Public Harm and Reputational Risk
- Fines and Penalties
- Legal Costs
- Cost of Notification

# Next Steps to Consider

- Conduct a robust Assessment with an Annual or Bi-Annual reassessment for compliance
- Determine Lines of Business affected by HIPAA
- Consider internal employee information in evaluation
- Map/Flow PHI movement within your organization, as well as flows to/from third parties
- Perform Data discovery to find all of your PHI
- Establish effective technical safeguards over PHI (encryption, access management, restriction for required use only)

# Conclusions & Final Thoughts

- **Plan ahead for impact of HIPAA across the organization**
  - Determine possible common responsibilities and oversight of IT, Information Security, and Internal Audit
  - Assess overlap between controls oversight and management
- **Determine control and safeguard catalogue for HIPAA prior to remediation – know what you're going after**
- **Engage impacted departments (IT, HR, Business, IA) early in the planning**
- **Assess your ability to combine HIPAA compliance activities with other compliance activities like PCI, (Unified Compliance), to increase the effectiveness & efficiency of your compliance programs**

KPMG

cutting through complexity

Michael D. Ebert
mdebert@kpmg.com