



**KPMG**  
cutting through complexity

## 2012 HIPAA Privacy and Security OCR Audits

Michael D. Ebert  
Partner, KPMG  
National HIPAA Services Leader

### 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

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	Safeguards	Consumer Control	Accountability	Public Responsibility
<ul style="list-style-type: none"> <li>• Information used only for intended purpose and only as much information as required for the intended purpose</li> <li>• Consumer use and disclosure statement</li> </ul>	<ul style="list-style-type: none"> <li>• Administrative, technical, and physical mechanisms to keep information private, confidential and secure within internal operating systems and external communications</li> </ul>	<ul style="list-style-type: none"> <li>• Informed consent to use information</li> <li>• Right to access and amend information</li> <li>• Authorization for disclosures</li> <li>• Record of disclosures</li> </ul>	<ul style="list-style-type: none"> <li>• Federal penalties for violations</li> <li>• Effective compliance activities to deter, identify, and punish violations</li> </ul>	<ul style="list-style-type: none"> <li>• Process for disclosing information for public health, research &amp; legal purposes</li> </ul>

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

2

Regulatory Background - Security Rule Standards

Administrative Procedures	Physical Safeguards	Technical Standards and Mechanisms (Data at rest & data in transit)
<ul style="list-style-type: none"> <li>■ Security Management Process</li> <li>■ Assigned Security Responsibility</li> <li>■ Workforce Security</li> <li>■ Information Access Management</li> <li>■ Security Awareness and Training</li> <li>■ Security Incident Procedures</li> <li>■ Contingency Plan</li> <li>■ Evaluation</li> <li>■ Business Associate Contracts and Other Arrangements</li> </ul>	<ul style="list-style-type: none"> <li>■ Facility Access Controls                             <ul style="list-style-type: none"> <li>- Disaster recovery</li> <li>- Emergency Mode</li> <li>- Equipment transfers</li> <li>- Facility security plan</li> <li>- Access Authorization process (physical access)</li> <li>- Maintenance records</li> <li>- Need to know access</li> <li>- Sign in and escort visitors</li> <li>- Testing and revision</li> </ul> </li> <li>■ Workstation Use</li> <li>■ Workstation Security</li> <li>■ Device and Media controls over hardware and software</li> </ul>	<ul style="list-style-type: none"> <li>■ Access and Authorization controls                             <ul style="list-style-type: none"> <li>- Context based, role based, or user based</li> <li>- Encryption</li> </ul> </li> <li>■ Audit controls (suspect access attempts)</li> <li>■ Integrity                             <ul style="list-style-type: none"> <li>- Data authentication</li> </ul> </li> <li>■ Personal and Entity Authentication                             <ul style="list-style-type: none"> <li>- Unique User ID</li> <li>- Authentication Technique                                     <ul style="list-style-type: none"> <li>PIN</li> <li>Token</li> <li>Biometric</li> <li>Call Back</li> </ul> </li> <li>- Automatic Logoff</li> </ul> </li> <li>■ Transmission Controls                             <ul style="list-style-type: none"> <li>- Access Controls</li> <li>- Audit Trail</li> <li>- Encryption</li> </ul> </li> </ul>

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

3

## 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 2011, so we are now standing up the program activities. The pilot audit program will be a three step process.

1. **Working with KPMG to develop the draft audit protocols.**  
Completed November 2011
2. **An initial round of audits tested the protocols. Results of field testing provided feedback for final protocol design.**  
Field work completed March 1<sup>st</sup>  
Final protocol design completed April 2012
3. **Rolling out the full range of audits and evaluation process.**  
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 than 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.

## 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

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

8

## Initial 20 Findings Analysis Overview

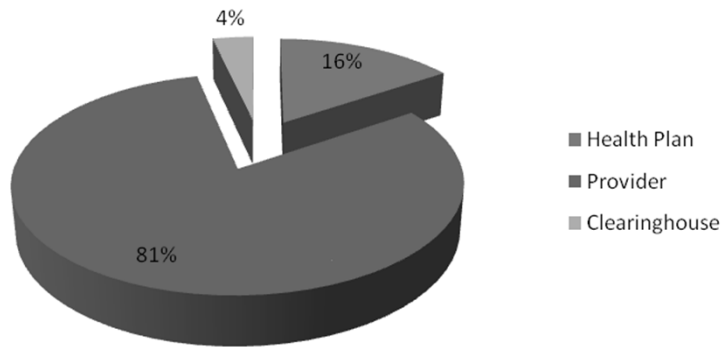


© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

9

### Initial 20 Findings Analysis Overview

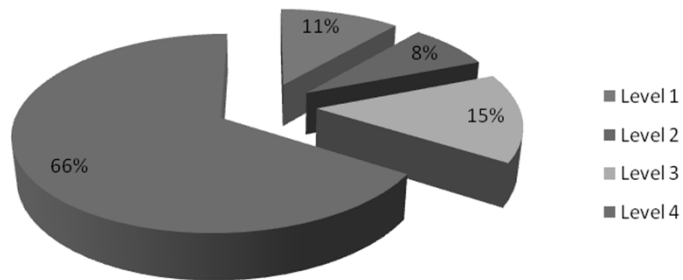
#### Analysis by Type of Covered Entity



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

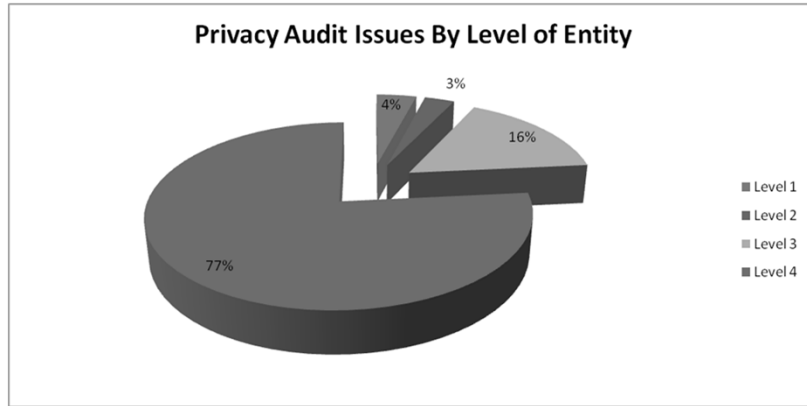
### Initial 20 Findings Analysis Overview

#### Analysis of Finding by Tier



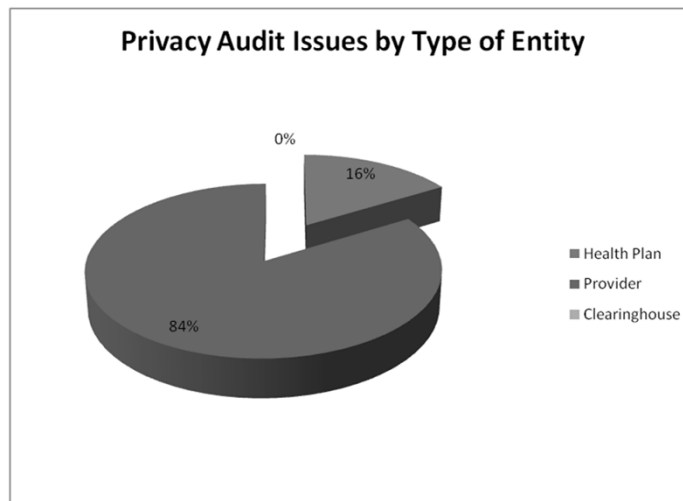
© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

### Initial 20 Findings Analysis Privacy Issues



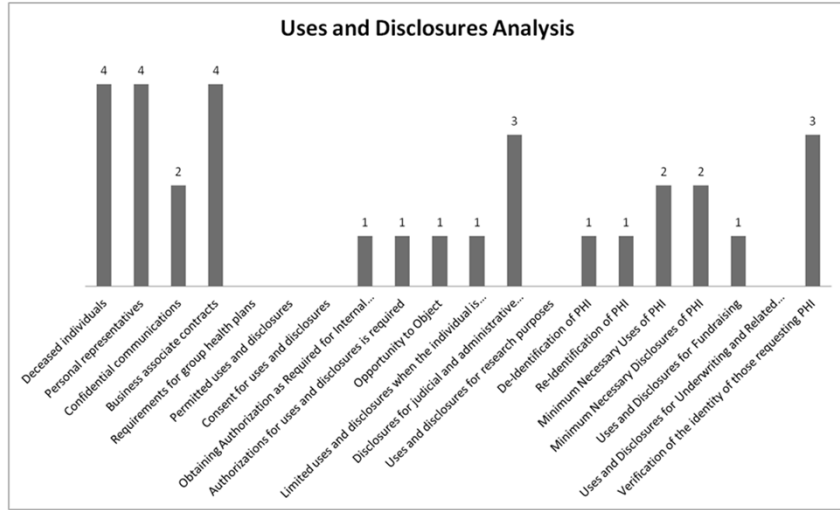
© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

### Initial 20 Findings Analysis Privacy Issues



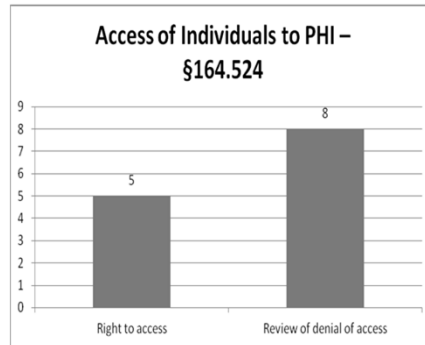
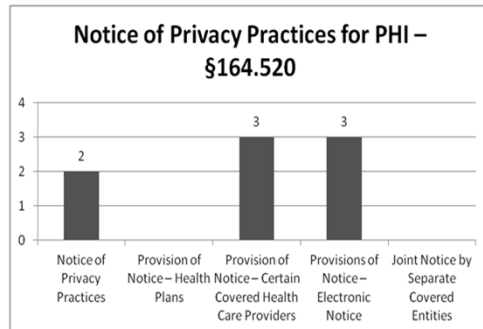
© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

**Initial 20 Findings Analysis Privacy: Uses and Disclosures**



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

**Initial 20 Findings Analysis Privacy: Notice and Access**



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

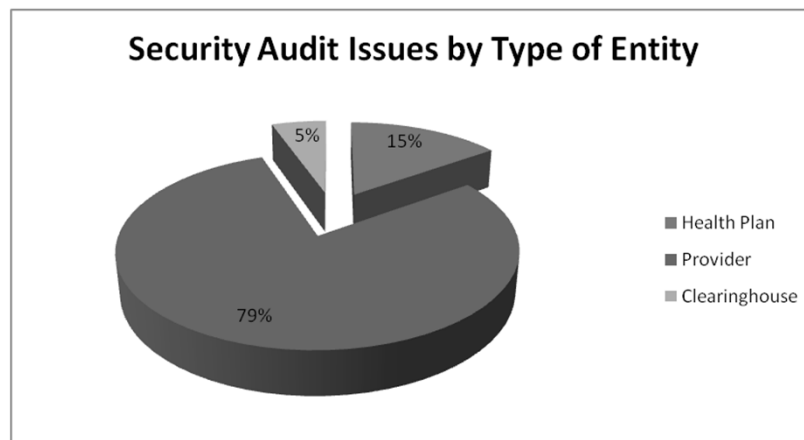


**Initial Findings Analysis Privacy: Administrative Requirements**



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

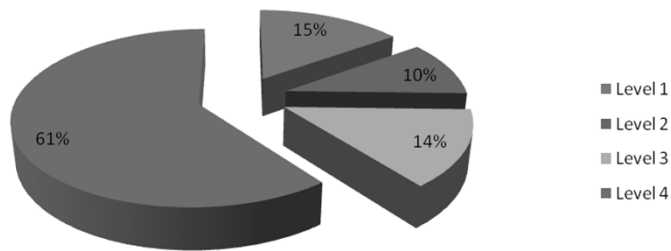
**Initial 20 Findings Analysis Security Issues**



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

**Initial 20 Findings Analysis Security Issues**

**Security Audit Issues by Level of Entity**

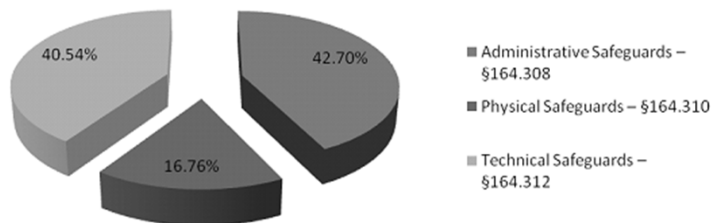


© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

18

**Initial 20 Findings Analysis Security Issues**

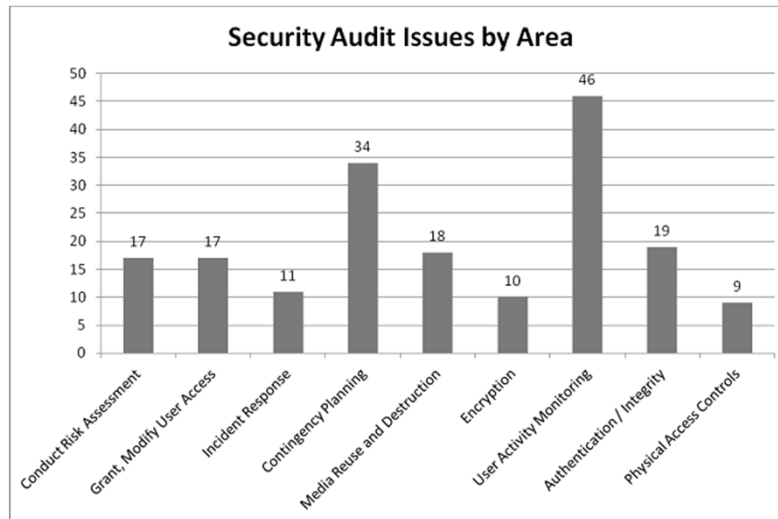
**Security Audit Issues by Area of HIPAA Security Rule**



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

19

## Initial 20 Findings Analysis Security Top Issues



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

20

## Preliminary Analysis

- **Policies and Procedures exist but are outdated or not implemented**
- **HIPAA compliance programs are not a priority**
- **Small providers are not in compliance**
- **Larger entities demonstrate security challenges**
- **Entities are not conducting Risk Assessments**
- **Entities are not managing third party risks**
- **Privacy challenges are widely dispersed throughout the protocol - no clear trends by entity type or size**

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

21

## 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**

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

24



Michael D. Ebert  
mdebert@kpmg.com

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 38075WDC

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.