OCR HIPAA Audit Readiness
ISACA - North Texas Chapter
April 11, 2013
Introduction

1. Basic components of HIPAA and HITECH legislation
2. HITECH and rising breaches
3. OCR HIPAA audits
4. Key findings of the pilot audits
5. Approaches to preparing for an OCR HIPAA audit
Basic components of HIPAA and HITECH legislation
## Introduction to healthcare relevant regulations

<table>
<thead>
<tr>
<th>Year</th>
<th>Relevant regulations</th>
</tr>
</thead>
</table>
| 1996 | - State regulations for sensitive health information  
      - HIPAA (Health Insurance Portability and Accountability Act) |
| 2000 | - State regulations for online environment  
      - State breach notification laws |
| 2004 | - Payment Card Industry standard  
      - State health regulations (beyond HIPAA)  
      - Genetic Information Nondiscrimination Act of 2008 |
| 2009 | - ARRA (American Recovery and Reinvestment Act)/HITECH Act (Health Information Technology for Economic and Clinical Health) |
| 2013 | - HIPAA Omnibus Rule |
Enacted in 1996 to protect health insurance coverage for workers and their families when they change or lose their jobs.

Administrative Simplification (AS) provisions require the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 updated several of HIPAA’s requirements and include more restrictive privacy protections over health information.

A Final rule updating the Privacy, Security, Enforcement, and Breach Notification rules was published in January 2013. It becomes effective March 26 and the compliance date is September 23, 2013.
HIPAA structure

- **Title I Portability**
  - Transaction Standards
    - Effective 10/16/2003
  - Code Set Standards
    - Effective 10/16/2003

- **Title II Administrative Simplification**
  - Unique Health Identifier Standards
    - Not Yet Final

- **Titles III, IV, and V**
  - Security Standards
    - Effective 4/2005
    - Administrative Procedures
    - Physical Safeguards
    - Technical Security Services
  - Privacy Standards
    - Effective 4/2003
    - Protected Health Information (PHI)
    - Major Components

**HIPAA/HITECH**

- Breaches
- Audits
- Findings
- Preparing
The Health Information Technology for Economic and Clinical Health (HITECH) Act signed on February 17, 2009 and the Final HIPAA rule issued on January 25th, 2013 changed and expanded the HIPAA privacy and security rules. Key impacts include:

- Breach notification
- Electronic health records
- Minimum necessary
- Disclosure limitations
- Deceased individuals
- Business associates & subcontractors
Key terms, definitions and references

► **Protected health information (PHI)** – any individually identifiable health information (IIHI) that is created, transmitted, or maintained by a covered entity.

► **Individually Identifiable Health Information (IIHI)** - Health information is individually identifiable if you can tell or could figure out to whom it refers by looking at it. Common identifiers include name, address, social security number, date of birth, Zip Code, and county.

► **Health information** - Health Information is broadly defined and includes any health information that pertains to a particular individual.

► **Covered Entities (CE)** - HIPAA applies only to covered entities. A covered entity might be a hospital, a physician practice, or any other provider who transmits health information in electronic form. Insurers and HMOs are also examples of covered entities.

► **Business associates (BA)** - One that creates, receives, maintains, or transmits PHI on behalf of a covered entity, namely:
  ▶ Health Information Organizations (HIOs)
  ▶ E-prescribing gateways
  ▶ Patient safety organizations
  ▶ Vendors of PHI that provide services,

Adapted From: [https://privacy.louisville.edu/Resources/Forms/hipaa-definitions.html](https://privacy.louisville.edu/Resources/Forms/hipaa-definitions.html)
There are all kinds of PHI in the world today.
There are many different organizations that house PHI.

- Payer organizations
- Provider organizations
- Output service
- Call centers
- Billing and claims processing
- Fraud investigation services
- Enrollment data repositories
- Systems supporting disease management services
- Member/patient services
- Systems and devices
The HIPAA Privacy Rule outlines notices, consents, and authorizations, individual rights, administrative requirements, uses and disclosures, and business associate relationships.

<table>
<thead>
<tr>
<th>Notices, Consents, and Authorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Rights</td>
</tr>
<tr>
<td>Administrative Requirements</td>
</tr>
<tr>
<td>Uses and Disclosures</td>
</tr>
<tr>
<td>Business Associate Relationships</td>
</tr>
</tbody>
</table>

**HIPAA/HITECH**

- Breaches
- Audits
- Findings
- Preparing
HIPAA privacy

- Business associate contracts
- Obtaining authorization
- De-identification of protected health information
- Minimum necessary requirements
- Notice
- Rights to request privacy protection for protected health information
- Confidential communications requirements
- Access of individuals to protected health information
- Amendment of protected health information

- Accounting of disclosures of protected health information
- Personnel designations
- Training
- Safeguards
- Complaints to the covered entity
- Sanctions
- Mitigation of harm
- Policies and procedures
- Retention

- Restrictions on sales and marketing
- Breach notification
The HIPAA Security Rule outlines requirements in administrative, physical, and technical safeguards.

I. Administrative

Actions, policies, and practices to manage the security measures needed to protect ePHI.

II. Physical

Physical measures, policies, and practices to protect buildings and computer equipments, from natural and environmental hazards, and unauthorized intrusion.

III. Technical

Policies and practices to govern the technologies that are used to access ePHI.
HIPAA security rule safeguards

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

► Physical
  ► Facility Access Controls
  ► Workstation Use
  ► Workstation Security
  ► Device and Media Controls

► Technical
  ► Access Control
  ► Audit Controls
  ► Integrity
  ► Person or Entity Authentication
  ► Transmission Security
HITECH and rising breaches
The penalties for breaches and HIPAA non-compliance has increased dramatically.

**Pre-HITECH**

- Penalty limited to $100 per violation or $25K for violation of a single standard in one year

**Post-HITECH**

- New Penalty Tiers:
  - Unknowing ($100 per violation/ $25K max)
  - Reasonable Cause ($1K per violation/$100K max)
  - Willful neglect ($10K per violation/$250K max)
  - Uncorrected willful neglect ($50K per violation/$1.5M max)

- Civil and criminal liability for certain HIPAA violations extended to business associates

- Mandatory investigations and civil penalties for violations due to willful neglect

- Increased emphasis on enforcement and significant funding to support that activity

---

**Non-Compliance Risks**

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

The OCR has stated that there are severe penalties and risks for non-compliance.
Why is the OCR taking this so seriously?

- Hacking/IT Incident
- Improper Disposal
- Loss
- Theft
- Theft, Loss
- Theft, Unauthorized Access/Disclosure
- Unauthorized Access/Disclosure
- Unknown
- Other

- 392 reported breaches from September 2009 – December 2011.
- Total number of records: 19,051,267.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
The majority of the reportable breaches relate to lack of information security controls.

Reported Breaches by Source

- Desktop Computer, 39, 15%
- Laptop Computer, 66, 25%
- Paper Records and Films, 56, 22%
- Network Server, 28, 11%
- Other, 15, 6%
- E-mail, 6, 2%
- Backup and Storage Media, 6, 2%
- Mailings, 4, 2%
- Portable Electronic Device, 40, 15%

= Lack of security controls

Adapted From: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
A leading healthcare company suffered a breach that proved costly.

- Lost a desktop computer containing 4.24 million members.
- 11 class action lawsuits have been consolidated into one case to “to maximize resources and avoid duplication of effort.”
- The total claim is $4.24 billion and represents damages in the amount of $1,000 per affected member.
- The breach was self reported under the provisions of the HITECH act.
- The theft covers two patient groups:
  - 3.3 million patients whose healthcare providers contract with Physician Services, mostly in the Bay Area, includes name, address, date of birth, phone, email, medical record number and health insurance provider.
  - 943,000 patients with doctors at Medical Foundation, most of them in the Sacramento area. In addition to the information above, the computer contains dates of service, descriptions of medical diagnoses and procedures from January 2005 to January 2011 for this group.

Industry Risk Examples - PII or PHI, it still needs to be secured.

**Physical theft of desktop PC**
- PII lost for ~3.3 million patients (names, addresses, DOB, phone numbers and email addresses)
- ePHI including medical diagnoses and procedures for about 943,000 patients exposed
- Two class action lawsuits filed, each for $1000/record: one for the total 4.2 million affected patients, another for the 943k who lost extensive information

**Physical theft of hard drives**
- 57 disk drives stolen from data closet of abandoned call center office
- Drives contained members’ name, address, ID number, SSN, DOB and diagnosis
- Remediation estimate of $16 million to encrypt data

**Vendor data loss from inadequate customer credentialing**
- Data for up to 500,000 individuals was compromised by fraudsters masquerading as legitimate businesses
- Settled lawsuit with Federal Trade Commission for $10 million fine and $5 million contingency fund; remediation costs too broad to quantify

**Loss of server hard disks**
- IBM misplaced 9 server hard disks during data center upgrade/move; PII, ePHI and financial information for 1.9 million customers was exposed
- Settled lawsuit with State of Connecticut for $250k fine and $500k contingency fund; remediation costs unknown

~$4 Billion+
~$16 Million
~$15 Million+
~$1 Million
In 2009, HITECH charged HHS OCR with proactive HIPAA enforcement.

- OCR Pilot Audit – About 115 audits were performed in 2011-2012

- In May 2012, OCR shared initial findings and Audit Protocol for HIPAA Security, Privacy & Breach Notification

- In December 2012, OCR completed pilot audit program. Enforcement totals exceeded $10.8M, OCR Director expects to continue.

- State AGs also have clear authority to pursue violations – most come from complaints and/or breaches.

- Department of Justice has explicit authority to pursue criminal cases against individual employees of health organizations.
The OCR recently released the audit protocol used in the pilot phase.

- There are two tables within the protocol:
  - Table 1 for HIPAA Security
  - Table 2 for HIPAA Privacy and Breach Notification

- The “Established Performance Criteria” column shows either the regulation language or an explanation of what is expected.

- The “Key Activity” column outlines what the covered entity should be doing to meet the requirement (e.g. developing awareness training, conduct risk assessment, etc.)

- The “Audit Procedures” outlines what the auditor will look for to prove compliance and implementation. A wide array of methods are referenced:
  - Inquiry: Interview management
  - Observation - Observe physical environment and covered entity practices
  - Examination: Collect, review and analyze supporting documentation
Upon notification, companies are generally given 10 days to prepare.

► OCR notifies covered entity in writing 30-days days prior to anticipated onsite site.

► Covered entity to provide requested information within 10 business days of the request for information.

► On site visit may take between 3-10 business days depending on the complexity of the organizations.

► Covered entity will have 10 business days to review and provide written comments to auditor on the final report.

► Final report to be completed and submitted to OCR within 30 business days after the covered entity’s response to draft copy.

Source: HHS Website
Documentation requests started high level and drilled deeper, especially into access.

The OCR had approximately 100+ total unique evidence requests. Initial requests for documentation primarily focused on:

► Information security policies and standards.
► HIPAA/security/privacy framework.
► HIPAA program governance (leadership, organization, roles/responsibilities).
► Access management procedures (provisioning, de-provisioning, periodic access reviews).
► HITECH breach notification policies and procedures.
► Other requests covering the safeguards and implementation specifications specified in the HIPAA security rule.
► Testing and evidence
The OCR provides a request list to obtain details across the covered entity.

- **Policy and procedures:**
  - HIPAA privacy and security policies and procedures
  - General privacy and security policies

- **Systems and processes:**
  - Listings of systems and processes that handle and process PHI
  - Testing documentation

- **Data protection compliance:**
  - Compliance and audit planning, assessment and reports
  - Contracts

- **General**
  - Organization chart
  - Training and awareness
The OCR protocol clearly conveys its intent to strictly enforce HIPAA requirements.

For example, one of the audit procedures calls for auditors to obtain and review:

- Screenshots from systems to determine whether technical access capabilities are defined (for read-only, full access, etc)
- Evidence of approval for workforce access to ePHI
- Evidence of risk assessment being performed to document position around the use and/or disclosure of ePHI
Key findings of the pilot audits
EY has received updates from the industry and information from several of our clients

The information contained in the following slides has been compiled based on our analysis of information obtained from:

- Our discussions with and analysis of the OCR audit program;
- Our clients who have completed the audit;
- OCR’s industry briefings;
- Our analysis and experience in implementing HIPAA programs.
The majority of the pilot audit covered entities had material findings.

Analysis of Findings by Rules

Security Audit Issues by Area

HIPAA/HITECH  Breaches  Audits  Findings  Preparing

Security
Privacy
Breach
Preparing for an OCR HIPAA audit
A defensible framework for building a HIPAA compliance program is critical.

- Out of the 29 original requests from the initial document request list, 17 (59\%) were access-related or partially access related.
- The requests emphasize the importance of an integrated governance model between the various requirements and stakeholders.
- OCR clearly examining roles, responsibilities and HIPAA governance.
- The OCR specifically made reference to reviewing "...any applicable industry guidance (e.g., studies, practices, regulations, etc.) or other reference material used to develop any of the policies and procedures requested below..." This emphasizes the importance of solid, defensible framework.
- OCR specifically discussed the completeness and accuracy of the application inventory of PHI data stores.
- The privacy and security requirements are clearly examined together rather than separately. Critical to have an integrated approach to addressing all safeguards.
Preparation is key. There are steps you can take to get ready...

► Implement a rigorous **risk assessment process** and be sure to revisit it at least yearly (or as major business impacts occur that would change your risk profile).

► Understand the **scope of your business affected by HIPAA**:
  - *Technology*: Applications, databases, servers
  - *Business*: Business units, geographies, functional areas

► Do not just look at member/subscriber/patient information; **pay attention to internal employee information** that is also considered PHI.

► Document and **map the flow of PHI** within your organization as well as externally to vendors, affiliates and business associates. It is critical to understand where the PHI is going.
  - If the flow of PHI is not known, perform an assessment to find the PHI data stores

► Implement effective **administrative, technical and physical safeguards** over PHI.

**Source:** Adapted from presentation of OCR/KPMG
Preparation is key. There are steps you can take to get ready…

► Larger organizations can have a difficult time governing its HIPAA program. Multiple stakeholders, processes, BU’s and risk inputs complicate the landscape and make testing and reporting difficult. **GRC technologies can streamline reporting and management of security and privacy risks.**

► **Vendor risk management** is critical. Third-parties are now considered a part of the extended enterprise and the borders of covered entities grow with each new business associate.

► **Strong incident management** processes are important to prove HITECH compliance.

► **Training, education and awareness** programs should be implemented as they are often the last line of defense over PHI protection.

► Understand **who has access to what**… Be sure to verify access on a periodic basis and remember: SOX may not care about “view access” but HIPAA does.

Source: Adapted from presentation of OCR/KPMG
Approaches to prepare for a HIPAA audit
Sample approaches to prepare for HIPAA compliance

1. OCR HIPAA Mock Audit
2. HIPAA Access Control Requirements Definition
3. Data at Rest Protection
4. HIPAA Security Acceleration Program
OCR HIPAA Mock Audit

► Initial request of HIPAA documents for which management will have 10 business days to provide:
  ► Scope of business affected by HIPAA (i.e., technology systems, covered entities, etc.)
  ► Information security policies and standards
  ► HIPAA/security/privacy framework
  ► HIPAA program governance (leadership, organization, roles/responsibilities)
  ► Access management procedures (provisioning, de-provisioning, periodic access reviews)
  ► HITECH breach notification policies and procedures

► Sample testing in higher risk areas, such as technical safeguards (e.g. user access, data encryption, unauthorized access, monitoring).

► A high-level findings and recommendations report
HIPAA Access Control Definition
Requirements for access controls were established using authoritative sources.

5 Authoritative Sources
- HITRUST
- COBIT 4.1
- NIST
- ISO/IEC 27002
- BITS

Requirements for access controls were established using authoritative sources.
Access management requirements are moving toward a unified control framework.

- Mapped the defined HIPAA Requirements to SOX and PCI Requirements.
- Mapped requirements (for the 3 regulations) are defined at a granular level to enable the development and deployment of actionable procedural guidance.

<table>
<thead>
<tr>
<th>Req. ID #</th>
<th>Requirement Attributes</th>
<th>Current Proposed HIPAA Requirements</th>
<th>SOX Requirements (SOX Compliance Manual)</th>
<th>PCI Requirements (PCI DSS 2.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1. Policies &amp; Procedures for provisioning access are updated when significant changes in the environment occur (e.g. organizational change, technology, etc). 2. Changes to policies and procedures require a revision date, updated version number, and approval from authorized approver. 3. Policies &amp; Procedures are reviewed no less than annually and approved as current by an authorized approver. 4. Policies &amp; Procedures are readily accessible to KP staff supporting the user access management processes. 5. All users (workforce members and non-workforce members) and non-users (system validation, etc.) that are allowed access to ePHI must be covered in the policies and procedures. Workforce members include employees, physicians, volunteers, trainees,</td>
<td>(84.305 a 4.100 - User Access Management policies and procedures for provisioning access to ePHI are documented, periodically reviewed, updated as needed, made available to those persons responsible for implementing the procedures and retained for 8 years from the date of their creation or the date when they last went in effect, whichever is later.</td>
<td>3.2.1 Checklist - Provisioning Requirements. Narratives, desktop procedures and other key process documents are approved at least annually by the BAO / Control Owner or formal designee.</td>
<td>12.1 Establish, publish, maintain, and disseminate a security policy. 12.1.1 Policy addresses PCI DSS requirements; 12.2 Daily operational security procedures that are consistent with the requirements are developed. 12.1.3 Policies and procedures are reviewed annually and updated when the environment changes.</td>
</tr>
</tbody>
</table>
Leveraged existing SOX Compliance Manual with HIPAA Updates to be piloted by “Dual applications”
Key Work Products

► HIPAA Access Control Requirements document.

► Mapped to SOX & PCI.

► HIPAA-SOX Access Control Compliance Manual for “Dual” Applications

► Vetted with Stakeholders – noted areas of impact

► Access Control Requirement Prioritization.

► Adapted SOX Tools and Enablers for “Dual” Applications
  ► Process Flows, Process Narratives, Job role templates, etc.
Data at Rest Protection
Data at Rest Protection – scope and approach

Layer 4
- Partner and Vendor hosted data

Layer 3
- Clinical IT (bio-medical) devices

Layer 2
- Applications (Database, E-mail, Business)
- Desktops and Laptops
- Mobile Devices
- Printers
- Removable Media (USB, CD-ROM, SD)

Layer 1
- Enterprise Storage - Online (Network Attached Storage and Storage Area Networks) and Offline (backup tapes)
- Servers

Project Approach…

1. Stakeholder Interviews
   Interviews to assess current state

2. Data Collection
   Data extraction and analysis

3. Create Roadmap
   Assess remediation costs and prioritize accordingly
Key References


► On-going information from OCR: http://www.hhs.gov/ocr/privacy/

► To view actual reported breaches: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
Thank you.

Michael D. Schultz
Manager
Dallas, Texas
Phone: +1 (214) 766-0804
E-Mail: michael.schultz@ey.com

Stacey Hamaker
Manager
Dallas, Texas
Phone: +1 (214) 384-4825
E-Mail: stacey.hamaker@ey.com