OCR/HHS HIPAA/HITECH Audit Preparation
Who are we

EHR 2.0 Mission: To assist healthcare organizations develop and implement practices to secure IT systems and comply with HIPAA/HITECH regulations.

- Education
- Consulting
- Toolkit(Tools, Best Practices & Checklist)

Goal: To make compliance an enjoyable and painless experience
Webinar Objective

Understand OCR/HHS HIPAA/HITECH audit program and steps required to prepare for an audit
Glossary

1. HHS, OCR, DOJ and SAG:

2. Covered Entity:

3. Assessment:

4. Findings:

5. Risk Analysis:
The American Recovery and Reinvestment Act of 2009 and HITECH

Federal Spending for ARRA includes federal tax cuts, expansion of unemployment benefits and other social welfare provisions, and domestic spending in education, health care, and infrastructure, including the energy sector.
HITECH Act

The Health Information Technology for Economic and Clinical Health ("HITECH") provisions of the American Recovery and Reinvestment Act of 2009 ("ARRA", also referred to as the "Stimulus Bill") codify and expand on many of the requirements contained in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations to protect the privacy and security of protected health information ("PHI").
HITECH modifications to HIPAA including:

- Creating incentives for developing a meaningful use of electronic health records
- Changing the liability and responsibilities of Business Associates
- Redefining what a breach is
- Creating stricter notification standards
- Tightening enforcement
- Raising the penalties for a violation
- Creating new code and transaction sets (HIPAA 5010, ICD10)
HIPAA Titles - Overview

HIPAA
Health Insurance Portability and Accountability Act

Title I
Health care Access, Portability and Renewability

Title II
Preventing Healthcare Fraud and Abuse
Medical Liability Reform
Administrative Simplification

Electronic Data Interchange
Privacy
Transactions
Identifiers
Code sets

Title III
Tax Related Health Provision

Title IV
Group Health Plan requirement

Title V
Group Offsets

Security
* Security Standards: General Rules
* Administrative Safeguard
* Physical Safeguard
* Technical Safeguard
* Organizational Requirements
* Policies and Procedures and Documentation Requirements
The two main rules of HIPAA are:

- **Privacy Rule**: Organizations must identify the uses and disclosures of protected health information (PHI) and put into effect appropriate safeguards to protect against an unauthorized use or disclosure of that PHI. When material breaches or violations of privacy are identified, the organizations must take reasonable steps to solve those problems in order to limit exposure of PHI.

- **Security Rule**: Defines the administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information.

(45 CFR Part 160 and Subparts A and C of Part 164)
HIPAA Security Rule

HIPAA Title II
Administrative Simplification

Security Standards: General Rules
(§164.306)

Administrative Safeguards
(§164.308)

Physical Safeguards
(§164.310)

Technical Safeguards
(§164.312)

Organizational Requirements
(§164.314)

Policies and Procedures
and Documentation Requirements
(§164.316)

- Security management process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation

- BA Contracts and other arrangements

- Facility Access Control
  - Workstation Use
  - Workstation Security
  - Device and Media Control

- Access Control
  - Audit Controls
    - Integrity
  - Person or entity authentication
  - Transmission Security
Information Security Model

Confidentiality
Limiting information access and disclosure to authorized users (the right people)

Integrity
Trustworthiness of information resources (no inappropriate changes)

Availability
Availability of information resources (at the right time)
Covered Entity

- HIPAA applies to any entity that is a

  - **Health care provider** - of services as a provider of medical or other health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business

  - **Health care clearinghouse** - public or private entity that does billing services, re-pricing companies, community health management information systems or community health information systems, etc

  - **Health plan** - means an individual or group plan that provides, or pays the cost of, medical care

Business Associates

- a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity’s workforce is not a business associate.

**Examples:**

- A *third party administrator* that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A *health care clearinghouse* that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An *independent medical transcriptionist* that provides transcription services to a physician.
- A *pharmacy benefits manager* that manages a health plan’s pharmacist network.
Enforcement Authorities

- Office for Civil Rights (OCR)
  - Investigating complaints filed with HHS
  - Impose civil money penalties
- Department of Justice (DOJ)
  - Investigates criminal violations
- State Attorney General (SAG)
  - Civil actions on behalf of state residents
  - Civil Money Penalties
OCR HITECH Audit

- KPMG to conduct 150 during 2012
- 20 scheduled during January – May 2012
  - In the pilot phase, OCR is auditing eight health plans, two claims clearinghouses plus 10 provider organizations, including three hospitals, three physicians' offices, and a laboratory, a dental office, a nursing/custodial facility and a pharmacy.
Sample letter

Date
Name of Entity
Address of Entity
Point of Contact of Entity

Dear Covered Entity:

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (45 CFR Part 160 and Part 164 Subparts C and E). These rules are designed to provide important health information privacy and security protections and rights for individuals. The OCR is committed to developing and enforcing strong health information privacy protections that do not impede access to quality health care.

The American Recovery and Reinvestment Act of 2009 (ARRA) requires HHS to audit covered entity and business associate compliance with the HIPAA privacy and security standards. To effectively implement this statutory mandate, OCR has engaged the services of a professional public accounting firm (KPMG LLP) to conduct performance audits, using generally accepted government auditing standards. You are receiving this letter because OCR has selected [Name of entity] to be the subject of an audit.

These audits are a new facet of the OCR health information privacy and security compliance program. Audits present an opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR’s established complaint investigations and compliance reviews. OCR will broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges. OCR will assess whether to open a separate compliance review in cases where an audit indicates serious compliance issues.
United States Government Accountability Office

By the Comptroller General of the United States

December 2011

Government Auditing Standards

2011 Revision
OCR Audit Timeline

Every covered entity and business associate is eligible for an audit.
OCR Audit Schedule

OCR: Audits are primarily a compliance improvement activity

From HHS.gov site
OCR enforces the Privacy and Security Rules in several ways:
1. by investigating complaints filed with it
2. conducting compliance reviews (audit) to determine if covered entities are in compliance
3. performing education and outreach to foster compliance with the rules' requirements
Resolution

OCR will attempt to resolve the case with the covered entity by obtaining:

1. Voluntary compliance
2. Corrective action which might include penalty
3. Resolution agreement
Common fallacies related to OCR audit

- “Our compliance officer handles everything – there’s no need to involve anyone else.” “We’re compliant; therefore, we’re secure.”
- “The last time we had an audit they didn’t find anything of concern.”
- “We have a security policy to keep our systems protected.”
- “Even if we mess up, the regulators aren’t going to come after us.”
Complaints Received by Calendar Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>8,524</td>
</tr>
<tr>
<td>2009</td>
<td>7,567</td>
</tr>
<tr>
<td>2008</td>
<td>8,706</td>
</tr>
<tr>
<td>2007</td>
<td>8,190</td>
</tr>
<tr>
<td>2006</td>
<td>7,340</td>
</tr>
<tr>
<td>2005</td>
<td>6,855</td>
</tr>
<tr>
<td>2004</td>
<td>6,534</td>
</tr>
<tr>
<td>Partial 2003</td>
<td>3,743</td>
</tr>
</tbody>
</table>
# Top 5 issues investigated

<table>
<thead>
<tr>
<th>Year</th>
<th>Issue 1</th>
<th>Issue 2</th>
<th>Issue 3</th>
<th>Issue 4</th>
<th>Issue 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Notice</td>
</tr>
<tr>
<td>2009</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Complaints to Covered Entity</td>
</tr>
<tr>
<td>2008</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Complaints to Covered Entity</td>
</tr>
</tbody>
</table>
OCR Compliance Audit Review

- Policies and procedures
- Risk Analysis and Mgmt.
- BA Agreement and Contracts
- Document-ation
- Training

OCR Compliance Audit
OCR Compliance Audit Review (Contd.)

- Off-site access and use of ePHI from remote locations
- Implementation of minimum necessary standard
- Storage of ePHI on portable devices and media
- Provision of Notices of Privacy Practices
- Disposal of equipment containing ePHI
- Executing proper authorization forms
- Physical security of facilities and mobile devices
- Technical safeguards in place to protect ePHI
- Data encryption
- Virus protection
- Monitoring of access to ePHI
# ePHI – 18 Elements

<table>
<thead>
<tr>
<th>Elements</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Max Bialystock</td>
</tr>
<tr>
<td>Address</td>
<td>1355 Seasonal Lane (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)</td>
</tr>
<tr>
<td>Dates related to an individual</td>
<td>Birth, death, admission, discharge</td>
</tr>
<tr>
<td>Telephone numbers</td>
<td>212 555 1234, home, office, mobile etc.,</td>
</tr>
<tr>
<td>Fax number</td>
<td>212 555 1234</td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:LeonT@Hotmail.com">LeonT@Hotmail.com</a>, personal, official</td>
</tr>
<tr>
<td>Social Security number</td>
<td>239-68-9807</td>
</tr>
<tr>
<td>Medical record number</td>
<td>189-88876</td>
</tr>
<tr>
<td>Health plan beneficiary number</td>
<td>123-ir-2222-98</td>
</tr>
<tr>
<td>Account number</td>
<td>333389</td>
</tr>
<tr>
<td>Certificate/license number</td>
<td>3908763 NY</td>
</tr>
<tr>
<td>Any vehicle or other device serial number</td>
<td>SZV4016</td>
</tr>
<tr>
<td>Device identifiers or serial numbers</td>
<td>Unique Medical Devices</td>
</tr>
<tr>
<td>Web URL</td>
<td><a href="http://www.rickymartin.com">www.rickymartin.com</a></td>
</tr>
<tr>
<td>Internet Protocol (IP) address numbers</td>
<td>19.180.240.15</td>
</tr>
<tr>
<td>Finger or voice prints</td>
<td>finger.jpg</td>
</tr>
<tr>
<td>Photographic images</td>
<td>mypicture.jpg</td>
</tr>
<tr>
<td>Any other characteristic that could uniquely identify the individual</td>
<td>28</td>
</tr>
</tbody>
</table>
Infrastructure

- Computers
- Storage Devices
- Networking devices (Routers, Switches & Wireless)
- Medical Devices
- Scanners, fax and photocopiers
- VoIP
- Smart-phones, Tablets (ipad, PDAs)
- Cloud-based services

Any device that electronically stores or transmits information using a software program
Trends in Healthcare IT

- Informatics
- Collaboration
- Mobile Computing
- EHR/HIE
Handheld Usage in Healthcare

- 25% usage with providers
- Another 21% expected to use
- 38% physicians use medical apps
- 70% think it is a high priority
- 1/3 use hand-held for accessing EMR/EHR

compTIA 2011 Survey
EMR and EHR systems

Figure 1. Percentage of office-based physicians with EMR/EHR systems: United States, 2001–2009, and preliminary 2010–2011

NOTES: EMR/EHR is electronic medical record/electronic health record. “Any EMR/EHR system” is a medical or health record system that is all or partially electronic (excluding systems solely for billing). Data for 2001–2007 are from the in-person National Ambulatory Medical Care Survey (NAMCS). Data for 2008–2009 are from combined files (in-person NAMCS and mail survey). Data for 2010–2011 are preliminary estimates (dashed lines) based on the mail survey only. Estimates through 2009 include additional physicians sampled from community health centers. Estimates of basic systems prior to 2006 could not be computed because some items were not collected in the survey. Data include nonfederal, office-based physicians and exclude radiologists, anesthesiologists, and pathologists.

SOURCE: CDC/NCHS, National Ambulatory Medical Care Survey.
Health Information Exchange (HIE)
Social Media

- How does your practice use it?
- How do your employees use it?
- Do you have policies?
Cloud-based services

- **Public Cloud**
  - EHR Applications
  - Private-label e-mail

- **Private Cloud**
  - Archiving of Images
  - File Sharing
  - On-line Backups

- **Hybrid**

Cloud Computing is taking all batch processing, and farming it out to a huge central or virtualized computers.

HIPAA regulations remain barriers to full cloud adoption.
Informatics

Informatics = People + Information + Technology
<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unencrypted laptop ePHI</td>
<td>Lack of auditing on EHR systems</td>
<td>Missing security patches on web server hosting patient information</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Unsecured wireless network in doctor’s office</td>
<td>Outdated anti-virus software</td>
<td>External hard drives not being backed up</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Sales presentation on USB thumb drive</td>
<td>Web server backup tape not stored in a secured location</td>
<td>Weak password on internal document server</td>
</tr>
</tbody>
</table>
Top 5 Recommendations to Survive an OCR Audit

1. Ensure **encryption** on all protected health information in storage and transit. (at least de-identification)
2. Implement a **mobile device security** program.
3. Strengthen information security user **awareness and training** programs.
4. Ensure that **business associate due diligence** includes clearly written contract, a periodic review of implemented controls.
5. **Minimize sensitive data** capture, storage and sharing.
Questions to your auditors

• Do you have an audit plan?

• Do you have detail audit objectives documented?

• Do you recommend action to correct deficiencies?
Effective Management of Security and Compliance

1. Find out where your business is weak
2. Determine the compliance and security needs & gaps
3. Put reasonable policies and business processes in place
4. Implement the right technologies & processes to help with enforcement
5. Re-evaluate on a periodic and consistent basis

Re-evaluate on a periodic and consistent basis

Determine the compliance and security needs & gaps

Implement the right technologies & processes to help with enforcement

Put reasonable policies and business processes in place
**HIPAA Security Checklist**

**Overview**

<table>
<thead>
<tr>
<th>HIPAA Security Rule Standard Implementation Specification</th>
<th>Implementation</th>
<th>Requirement Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>Required</td>
<td>Policies and procedures to manage security violations</td>
<td>Penetration test, vulnerability assessment</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Required</td>
<td>Conduct vulnerability assessment</td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td>Required</td>
<td>Implement security measures to reduce risk of security breaches</td>
<td>SIM/SEM, patch management, vulnerability management, asset management, helpdesk</td>
</tr>
<tr>
<td>Sanction Policy</td>
<td>Required</td>
<td>Worker sanction for policies and procedures violations</td>
<td>Security policy document management</td>
</tr>
<tr>
<td>Information System Activity Review</td>
<td>Required</td>
<td>Procedures to review system activity</td>
<td>Log aggregation, log analysis, security event management, host IDS</td>
</tr>
<tr>
<td>Assigned Security Responsibility</td>
<td>Required</td>
<td>Identify security official responsible for policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Workforce Security</td>
<td>Required</td>
<td>Implement policies and procedures to ensure appropriate PHI access</td>
<td></td>
</tr>
<tr>
<td>Authorization and/or Supervision</td>
<td>Addressable</td>
<td>Authorization/supervision for PHI access</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Workforce Clearance Procedure</td>
<td>Addressable</td>
<td>Procedures to ensure appropriate PHI access</td>
<td></td>
</tr>
<tr>
<td>Termination Procedures</td>
<td>Addressable</td>
<td>Procedures to terminate PHI access security policy document management</td>
<td></td>
</tr>
<tr>
<td>Information Access Management</td>
<td>Addressable</td>
<td>Procedures to terminate PHI access security policy document management</td>
<td>Background checks</td>
</tr>
<tr>
<td>Isolation Health Cleaeninghouse Functions</td>
<td>Required</td>
<td>Policies and procedures to authorize access to PHI operations</td>
<td>Single sign-on, identity management, access controls</td>
</tr>
<tr>
<td>Access Authorization</td>
<td>Addressable</td>
<td>Policies and procedures to authorize access to PHI</td>
<td>Application proxy, firewall, mandatory UPN, SOCKS</td>
</tr>
<tr>
<td>Access Establishment and Modification</td>
<td>Addressable</td>
<td>Policies and procedures to separate PHI from other operations</td>
<td></td>
</tr>
<tr>
<td>Security Awareness Training</td>
<td>Addressable</td>
<td>Policies and procedures to authorize access to PHI</td>
<td>Mandatory, discretionary and role-based access control</td>
</tr>
<tr>
<td>Training program for workers and managers</td>
<td>Required</td>
<td>Policies and procedures to grant access to PHI</td>
<td>Security policy document management</td>
</tr>
<tr>
<td>HIPAA Checklist</td>
<td></td>
<td>Training program for workers and managers</td>
<td></td>
</tr>
</tbody>
</table>
EHR 2.0 Toolkit for Planning & Documentation

● http://ehr20.com/toolkit/
Key Takeaways

- HITECH act enforces HIPAA guidelines with new audit, penalties, notifications requirements etc.,

- ePHI elements drives the security and compliance requirements

- There is no silver bullet for audit issues. It is a journey of continuous assessment and improvement
How can you help us?

- Follow-us on social media
  
  facebook.com/ehr20 (Like)
  
  linkedin.com/company/ehr-2-0 (Follow us)
  
  https://twitter.com/#!/EHR_20 (Follow)

- Next Webinar on Meaningful Use Risk Analysis (3/14)


We sincerely appreciate your referrals!
Thank you!!