Game Changers: Omnibus Rule Overview & OCR Audits
HFMA Lone Star

Presented by Mac McMillan
CEO, CynergisTek, Inc.

Today’s Presenter

- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- Chair, HIMSS P&S Steering Committee
- HIT Exchange Editorial Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- HealthTech Industry Advisory Board
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired
Agenda

• The Omnibus Rule
  – Breach Notification
  – Business Associates
  – Privacy Updates
  – Enforcement Changes
• 2012 OCR Audits
  – The Audit Process
  – The Audit Protocol
  – Lessons Learned
• Questions
Omnibus Is Here

- The American Recovery & Reinvestment Act 2009, identifies several changes to the Privacy & Security Rules
- Effective date for all provisions is March 26, 2013
- Enforcement date for most provisions is September 23, 2013
- Business Associate agreements in force prior to January 25, 2013 may be grandfathered until September 23, 2014

Multiple Changes

- Implements elements of the HITECH Act
- Incorporates underwriting nondiscrimination of GINA
- Implements changes to breach, privacy, security and enforcement rules
- Minor deviations from proposed rule
- Does not address Minimum Necessary, Accounting for Disclosures or changes to SAMHSA, CLIA or Common Rules
Breach Notification

- An impermissible acquisition, access, use or disclosure of protected health information
- Presumed to be reportable
- Unless the entity can demonstrate through risk analysis that there is a low probability that protected health information has been compromised
- Risk of Harm consideration is removed

Breach Notification

- To demonstrate low probability of compromise entity must
- Document a risk analysis
- Four factors of consideration:
  - The nature and extent of PHI involved
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent of mitigation present
- Other factors may also be considered
Breach Notification

- Notifications of breaches affecting 500 or more
  - Without undue delay within 60 days of discovery
- Notifications of breaches affecting less than 500
  - Within 60 days of the end of the calendar year in which the breach was discovered
  - Looking at options to make submissions easier

Privacy Updates

- Expanded categories (department, Treating physician, Outcomes, Insurance status) of PHI that may be used for fundraising with greater and more restrictive provisions for opting out and notification as part of NPP
- Expanded definition of what uses and disclosures are considered marketing and therefore require authorization, tied to financial remuneration
- Omnibus generally prohibits an entity from receiving payment for PHI without consent, certain exceptions apply
- Omnibus introduces multiple changes to what is permitted under authorizations for research
Privacy Updates

• Omnibus limits application of HIPAA to decedent information (50 yrs) and communications with individuals involved with the decedent after death
• Relaxed requirements around disclosure of student immunization records
• Omnibus defines genetic information as health information and applies protections to include prohibition for a health plan to use such information in underwriting

Privacy Updates

• Omnibus provides for expanded Rights of Access and to request restrictions
  — Expands the right to an electronic copy of any PHI stored electronically in a designated record set
  — The preamble of the rule states that entities will need to invest in additional technology to meet this requirement
  — Individual has a right to direct the information be sent to another individual
  — Information may be transmitted using unencrypted email so long as entity warns the recipient of the risks
  — Provides 30 days fewer to provide information (30/30 rule)
• Provides for restrictions of access to information if individual pays in cash and in full
• Places responsibility for telling subsequent providers of the restrictions on the individual not the hospital
• Updates to Notice of Privacy Practice required
Notice of Privacy Practices

- Duty to notify individuals of breach of unsecured PHI
- May not refuse to restrict access to record when patient pays in full in cash
- May contact for fundraising with right to opt out of fundraising communications
- Plans: restriction from using or disclosing genetic information for underwriting purposes
- Deletion of appointment reminders or treatment options
- Types of uses and disclosures requiring authorization
- Statement concerning uses and disclosures for marketing or sale of PHI
- Statement that other uses and disclosures will only be made with authorization
- Statement that patients may revoke authorization

Business Associates

- Expands definition of Business Associate to any organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity
- Also identifies subcontractors, patient safety organizations, health information organizations, e-prescribing gateways and vendors of personal health records
- Omnibus makes business associates directly liable
- Omnibus makes CEs and BAs responsible for the actions of their “Agents”
- Omnibus reminds CEs to use Business Associate Agreements, but makes it clear that BAs are liable regardless
- Provides definitions around timeline requirements for updating BAAs
Business Associates: The 6 Commandments

- Must observe rules regarding uses and disclosures
- Must make notification to CE in case of a breach
- Must provide an e-copy of PHI if requested as specified in contract
- Must disclose PHI to HHS when conducting a compliance review/investigation
- Must provide an accounting for disclosure
- Must comply with the HIPAA Security & Privacy rules

Enforcement

- Business Associates (including their subcontractors) now are subject to civil money penalties and other enforcement actions for noncompliance with applicable provisions of HIPAA, including violations by their agents.
- Omnibus Rule retains the definition of willful neglect as “conscious, intentional failure or reckless indifference to the obligation to comply” with HIPAA.
- Requirement to proceed to informal resolution first removed.
Enforcement

- Omnibus redefines reasonable cause for determination of penalties:
  - The nature and extent of any violation, including the number of individuals affected and the duration of the violation;
  - The nature and extent of any individual's resulting physical, financial, or reputational harm, including any hindrance to the individual's ability to obtain health care;
  - The history of prior noncompliance, including similar prior indications of non-compliance and the offending party's responses to them;
  - The financial condition of the offending party, including difficulties that could have affected compliance or that could cause a money penalty to jeopardize the future provision of health care; and
  - Such other matters as justice may require.

Background: The Audit Program
HITECH: Establishes Requirement

- The American Recovery & Reinvestment Act 2009, in Section 13411, requires HHS to conduct periodic audits to ensure covered entities and business associates are meeting HIPAA compliance requirements.
- To begin this audit process HHS launches pilot program.
- The OCR Random Audit Program commenced FY 2012 and initial audits will be completed by CY 2012.

Categories

Level 1 Entities
- Large Provider / Health Plan
- Extensive use of HIT - complicated HIT enabled clinical /business work streams
- Revenues and or assets greater than $1 billion

Level 2 Entities
- Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company
- Paper and HIT enabled work flows
- Revenues and or assets between $300 million and $1 billion

Level 3 Entities
- Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don’t adjudicate their claims
- Some but not extensive use of HIT – mostly paper based workflows
- Revenues between $50 million and $300 million

Level 4 Entities
- Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)
- Little to no use of HIT – almost exclusively paper based workflows
- Revenues less than $50 million
## Entities Selected

<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Plans</td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>11</td>
<td>47</td>
</tr>
<tr>
<td>Healthcare Providers</td>
<td>11</td>
<td>16</td>
<td>10</td>
<td>24</td>
<td>61</td>
</tr>
<tr>
<td>Healthcare Clearinghouses</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>26</strong></td>
<td><strong>31</strong></td>
<td><strong>22</strong></td>
<td><strong>36</strong></td>
<td><strong>115</strong></td>
</tr>
</tbody>
</table>

## The Audit Process
The Audit Timeline

- Notification letter sent to Covered Entity: 1 Day
- On-site field work: Min. 15 Days
- Covered Entities review and comment on draft audit report: 3-10 Days, 20-30 Days, 10 Days, 30 Days
- Receiving and reviewing documentation and planning the audit field work
- Draft audit report
- Final audit report

Notification

- Phone call to confirm name and address for letter.
- Notification by registered mail 30 – 90 days in advance. Includes letter from OCR providing basis for audit under HITECH and introduces the audit process.
- The letter is addressed to the CEO so organizations need to redirect it as soon as it arrives.
- Follow up call to confirm receipt.
- Timing for audit activities tied to date organization receipts for letter.
Submit Documentation

- List of documents is provided at attachment to the Notification letter.
- List of items such as policies, procedures, plans, assessments, demographic information, forms, etc.
- Information is due within 15 business days of receipt of the Notification letter.
- Important to provide as much as possible.

On-Site Data Collection

- On-site field activities can begin 20 – 60 days from notification.
- On-site data collection can last from 3 – 10 business days and involve up to 5 auditors.
- The on-site visit will include interviews of key personnel, other staff members, site walkthroughs, operational reviews, and requests for further information.
- On-site activities will include entrance/exit conferences.
- General focus for audit is provided, but audits are not scripted.
**Post On-Site Activity**

- The Audit team will take 20 – 30 days following the on-site visit to produce a draft report.
- The site can expect additional questions/requests for information while the report is being written.
- Report will include a Letter of Representation, spreadsheet with list of findings/observations.
- Upon completion the draft report is provided to the site. It includes site information, findings/observations, recommendations, and request for response.

**Draft Report & Response**

- The site has 10 business days from the date of receipt of the report to review and provide a response to deficiencies noted.
- Site should review the report closely, identify clarifying questions, mitigating information, and plans for remediation.
- Site should take full advantage of expert advise from consultants and legal when developing response.
Final Report & Disposition

- Auditors have up to 30 days to finalize report.
- Final report and site responses forwarded to OCR.
- OCR determines final disposition, provides report to audited entity.
- OCR reserves the right to conduct follow up review or investigate where circumstances warrant.

The Audit Protocol
Audit Procedures

- Current # 169, subject to change
- 78 Privacy audit procedures
- 81 Security audit procedures
- 10 Breach notification procedures
- hhs.gov/ocr

Example Audit Procedure

- §164.312(a)(1) **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
Example Audit Procedure

- **Inquire** of management...
- **Obtain** and review policies and procedures...
- Obtain and **review evidence/documentation**...
- If CE has chosen not to fully implement, then must have **documentation of why**...
Interesting Observations

- 10% of selectees had no audit findings, 10% of selectees were totally unprepared for audit
- Security accounted for more than 60% of audit findings
- Providers had greatest proportion of findings – 65%
- Smallest entities struggled the most in all three areas
- Significantly fewer findings for those entities who fully implemented addressable specifications
- Most common excuse heard for non-compliance – “unaware of the requirement”
- Lack of application of sufficient resources, incomplete implementation, complete disregard

Overall Outcomes
Lessons Learned Overall

- By Rule
- By Level
- By Type

Privacy Outcomes by Issue
Privacy Outcomes by Function

Security Outcomes by Issue
Top Areas of Concern

• Privacy
  – Notice of privacy practices
  – Access of individuals
  – Minimum Necessary, and
  – Authorizations

• Security
  – Risk analysis
  – Access control
  – Contingency planning
  – Media movement and disposal, and
  – Audit controls and monitoring

Wrap Up & Questions
What’s Next

• Complete OCR audit program evaluation, all elements
• Requesting feedback from audited organizations
• Creating webpage on OCR site for identifying best practices
• Identify changes to program elements and update process and protocol
• Develop technical assistance for industry based on results of audits
• Determine where follow up is appropriate

Thank You

Mac McMillan
Mac.McMillan@cynergistek.com
(512) 402-8555
www.cynergistek.com