Lessons Learned from HIPAA Audits

October 29, 2012

Tony Brooks, CISA, CRISC
Partner - IT Assurance and Risk Services
HORNE LLP
AGENDA

- HIPAA/HITECH Regulations
- Breaches and Fines
- OCR HIPAA/HITECH Compliance Audit Initial Findings
- HORNE HIPAA/HITECH Compliance Audit Findings
- What You Should Be Doing
HIPAA/HITECH REGULATIONS
Current Status of HIPAA/HITECH Regulations

- HITECH Act (2009)
  - Established breach notification requirements
  - Established new penalty Levels
  - Established compliance requirements for business associates
  - Extended enforcement authority to state attorneys general
  - Mandated performance of privacy and security audits
Current Status of HIPAA/HITECH Regulations

- HITECH Act (2009)
  - Requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards
  - To implement this mandate, OCR is piloting a program to perform up to 115 audits of covered entities to assess HIPAA privacy, security and breach notification performance
  - Audits are being conducted in two phases
    a. Initial pilot audits to test the newly developed protocol
    b. Final pilot audits through December 2012
Current Status of HIPAA/HITECH Regulations

- HIPAA/HITECH Act Omnibus Final Rule Not Finalized
  - OMB has extended review of the rule under EO12866
  - The Omnibus rule is expected to include modifications to:
    a. The Breach Notification Rule
    b. The HIPAA Enforcement Rule, implementing changes mandated by the HITECH Act
    c. The Privacy and Security Rules, implementing changes mandated by the HITECH Act, as well as other changes to the Privacy Rule proposed in July 2010
    d. The Privacy Rule, implementing changes required by the Genetic Information Nondiscrimination Act
BREACHES AND FINES
FOR IMMEDIATE RELEASE
March 13, 2012

HHS settles HIPAA case with BCBST for $1.5 million

First enforcement action resulting from HITECH Breach Notification Rule

Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. Leon Rodriguez, Director of the HHS Office for Civil Rights (OCR), announced today. BCBST has also agreed to a corrective action plan to address gaps in its HIPAA compliance program. The enforcement action is the first resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule.

The investigation followed a notice submitted by BCBST to HHS reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the protected health information (PHI) of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR’s investigation indicated BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

“This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program,” said OCR Director Leon Rodriguez. “The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients’ right to private and secure health information.”

In addition to the $1,500,000 settlement, the agreement requires BCBST to review, revise, and maintain its Privacy and Security Rules.
BCBST Breach

What Happened?

✓ 57 unencrypted computer hard drives were stolen from a leased facility with PHI of over 1 million individuals

What Were The Findings?

✓ Failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes

✓ Failed to implement appropriate physical safeguards by not having adequate facility access controls
FOR IMMEDIATE RELEASE
June 26, 2012

Alaska settles HIPAA security case for $1,700,000

The Alaska Department of Health and Social Services (DHSS) has agreed to pay the U.S. Department of Health and Human Services’ (HHS) $1,700,000 to settle possible violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. Alaska DHSS has also agreed to take corrective action to properly safeguard the electronic protected health information (ePHI) of their Medicaid beneficiaries.

The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by Alaska DHSS as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The report indicated that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of a DHSS employee. Over the course of the investigation, OCR found evidence that DHSS did not have adequate policies and procedures in place to safeguard ePHI. Further, the evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.

In addition to the $1,700,000 settlement, the agreement includes a corrective action plan that requires Alaska DHSS to review, revise, and maintain policies and procedures to ensure compliance with the HIPAA Security Rule. A monitor will report back to OCR regularly on the state’s ongoing compliance efforts.

“Covered entities must perform a full and comprehensive risk assessment and have in place meaningful access controls to safeguard hardware and portable devices,” said OCR Director Leon Rodriguez. “This is OCR’s first HIPAA enforcement action against a state agency and we expect organizations to comply with their obligations under these rules regardless of whether they are private or public entities.”

Alaska DHHS Breach

- What Happened?
  ✓ A USB hard drive possibly containing ePHI was stolen from the vehicle of an employee
- What Were The Findings?
  ✓ Did not have adequate policies and procedures in place
  ✓ Had not completed a risk analysis
  ✓ Had not implemented sufficient risk management measures
  ✓ Had not completed security training for its workforce members
  ✓ Had not implemented device and media controls
  ✓ Had not addressed device and media encryption
FOR IMMEDIATE RELEASE
September 17, 2012

Massachusetts provider settles HIPAA case for $1.5 million

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (collectively referred to as "MEEI") has agreed to pay the U.S. Department of Health and Human Services (HHS) $1.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. MEEI also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its patients’ protected health information.

The investigation by the HHS Office for Civil Rights (OCR) followed a breach report submitted by MEEI as required by the Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification Rule, reporting the theft of an unencrypted personal laptop containing the electronic protected health information (ePHI) of MEEI patients and research subjects. The information contained on the laptop included patient prescriptions and clinical information.

OCR’s investigation indicated that MEEI failed to take necessary steps to comply with certain requirements of the Security Rule, such as conducting a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices, implementing security measures sufficient to ensure the confidentiality of ePHI that MEEI created, maintained, and transmitted using portable devices, adopting and implementing policies and procedures to restrict access to ePHI to authorized users of portable devices, and adopting and implementing policies and procedures to address security incident identification, reporting, and response. OCR’s investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the Security Rule.

"In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices," said OCR Director Leon Rodriguez. "This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom."

Massachusetts Eye and Ear Infirmary

- What Happened?
  ✓ An unencrypted personal laptop containing patient prescriptions and clinical information.

- What Were The Findings?
  ✓ Had not conducted a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices
  ✓ Had not implemented security measures sufficient to ensure the confidentiality of ePHI created, maintained, and transmitted using portable devices
  ✓ Had not adopted and implemented policies and procedures to restrict access to ePHI to authorized users of portable devices
OCR HIPAA/HITECH COMPLIANCE AUDIT INITIAL FINDINGS
OCR HIPAA/HITECH Audit Program

- How the program works
  - Entities selected for an audit receive a notification letter from OCR and asked to provide documentation to the auditor
  - Every audit includes a site visit and result in an audit report
  - Audit report states
    a. How the audit was conducted
    b. What the findings were
    c. What actions the covered entity is taking in response to those findings
OCR HIPAA/HITECH Audit Program

- **Purpose of the audits**
  - Measure performance against established criteria
  - The Rules were made auditable and measureable by developing performance criteria to execute these audits
  - Conducted under GAGAS, Generally Accepted Government Auditing Standards (aka, Yellow Book Standards)
  - Renders an opinion of whether entity has key controls and processes to allow entity to maintain or achieve compliance with the Rules
  - Not intended to be punitive, but rather measure compliance with regulations
OCR HIPAA/HITECH Audit Program

- Goals for the Audit Program
  - Examine mechanisms for compliance
  - Understand how industry is complying with the regulations
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Encourage renewed attention to compliance activities
OCR HIPAA/HITECH Audit Program

- Audit protocol was released on June 26, 2012
  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

  ✓ Covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.

  ✓ Covers Security Rule requirements for administrative, physical, and technical safeguards

  ✓ Covers requirements for the Breach Notification Rule.
## OCR HIPAA/HITECH Audit Program

<table>
<thead>
<tr>
<th>Section</th>
<th>Established Performance Criteria</th>
<th>Key Activity</th>
<th>Audit Procedures</th>
</tr>
</thead>
</table>
| §164.308 | §164.308(a)(1): Security Management Process §164.308(a)(1)(ii)(a) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | Conduct Risk Assessment | • Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.  
• Obtain and review relevant documentation and evaluate the content relative to the specified criteria for an assessment of potential risks and vulnerabilities of ePHI.  
• Evidence of covered entity risk assessment process or methodology considers the elements in the criteria and has been updated or maintained to reflect changes in the covered entity's environment.  
• Determine if the covered entity risk assessment has been conducted on a periodic basis.  
• Determine if the covered entity has identified all systems that contain, process, or transmit ePHI. |
OCR HIPAA/HITECH Audit – Initial Findings

- The initial audit phase involved the identification of 20 covered entities (10 providers, 8 health plans and 2 health clearinghouses) to audit.
  - Level 1 entities – large provider or plan with over $1 billion in revenues and extensive HIT use
  - Level 2 entities – regional providers or plans with revenues between $300 million to $1 billion with paper and HIT enabled workflows
  - Level 3 entities – community hospitals, regional pharmacies, self-insured health plans that do not adjudicate their own plans with $50-$300 million in revenues and some HIT use
  - Level 4 entities – small providers, community hospitals or rural pharmacy with revenues less than $50 million and little to no use of HIT
OCR HIPAA/HITECH Audit – Initial Findings

- **General Findings**
  - More organizations had trouble with security compliance than privacy compliance
  - Smaller organizations had more difficulties establishing HIPAA compliance programs than larger organizations
  - Many organizations have failed to conduct regular risk assessments
  - Many organizations are not paying enough attention to third party risks, including business associate compliance
OCR HIPAA/HITECH Audit – Initial Findings

- Top Privacy Issues
  - PHI uses and disclosures related to deceased individuals
  - PHI uses and disclosures related to personal representatives
  - Business associate contracts
  - Disclosures for judicial and administrative proceedings
  - Verification of the identity of an individual requesting PHI
OCR HIPAA/HITECH Audit – Initial Findings

- Top Security Issues
  - User Activity Monitoring
  - Contingency Planning
  - Authentication and integrity
  - Media Reuse and Destruction
  - Conducting risk assessments
  - Granting and/or modifying user access
OCR HIPAA/HITECH Audit – Initial Findings

- **OCR Recommendations**
  - Conduct a robust HIPAA compliance review and risk assessment
  - Identify Lines of Business affected by HIPAA
  - Map PHI flows within the organization as well as flows to and from third parties
  - Identify all of your organization’s PHI
  - Seek guidance available on OCR website
HORNE
HIPAA/HITECH COMPLIANCE
AUDIT FINDINGS
### Example Audit Findings

#### Policies and Procedures

<table>
<thead>
<tr>
<th>Finding</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual review and update of P&amp;P not performed</td>
<td></td>
</tr>
<tr>
<td>Formal separate P&amp;P needed for Self Funded Health Plan</td>
<td></td>
</tr>
<tr>
<td>P&amp;P should address the distribution and recovery of keys</td>
<td></td>
</tr>
<tr>
<td>P&amp;P should address the use of shredders and shred bins</td>
<td></td>
</tr>
<tr>
<td>Most recent version of Notice of Privacy Practices is not used</td>
<td>throughout the organization</td>
</tr>
<tr>
<td>Updated Business Associate Agreements have not been received for some</td>
<td>major vendors</td>
</tr>
<tr>
<td>major vendors</td>
<td></td>
</tr>
</tbody>
</table>
Example Audit Findings

<table>
<thead>
<tr>
<th>Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal Risk Management Process should be established</td>
</tr>
<tr>
<td>Detailed PHI systems inventory should be produced and updated annually</td>
</tr>
<tr>
<td>Formal periodic review of information systems should be performed to determine viability of systems and vendors</td>
</tr>
<tr>
<td>Periodic access rights reviews should be performed for all systems and applications</td>
</tr>
<tr>
<td>Information systems activity should be reviewed on a regular basis</td>
</tr>
</tbody>
</table>
**Example Audit Findings**

<table>
<thead>
<tr>
<th>Disclosure and Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussions with patients concerning PHI can be overheard</td>
</tr>
<tr>
<td>Some computer screens are not positioned for privacy</td>
</tr>
<tr>
<td>Some computers do not use screen saver passwords</td>
</tr>
<tr>
<td>Documents to be shredded left in boxes under desks</td>
</tr>
<tr>
<td>Patient charts and medical information viewable by unauthorized personnel and left unsecured, often overnight</td>
</tr>
<tr>
<td>Mail containing PHI is left unsecured in mail boxes</td>
</tr>
<tr>
<td>Returned meal trays may have meal cards containing patient information on them which are thrown in the trash</td>
</tr>
</tbody>
</table>
### Example Audit Findings

**Disclosure and Access (continued)**

<table>
<thead>
<tr>
<th>Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-rays or MRI's brought and left behind by patients are sent to Lost and Found</td>
</tr>
<tr>
<td>Faxes left on machines, sometimes for days</td>
</tr>
<tr>
<td>Communications with ambulances is not secure</td>
</tr>
<tr>
<td>Laptops and other portable devices containing ePHI are not encrypted</td>
</tr>
<tr>
<td>Laptop capable of storing ePHI was left unsecured in an unoccupied office</td>
</tr>
<tr>
<td>Email transmission of ePHI is not always encrypted</td>
</tr>
</tbody>
</table>
Example Audit Findings

<table>
<thead>
<tr>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal patch management policy needed</td>
</tr>
<tr>
<td>Formal change management policy needed</td>
</tr>
<tr>
<td>Wireless system security should be updated to more secure WPA-2 or WPA-PSK authentication methods</td>
</tr>
<tr>
<td>Some application systems utilize generic user IDs</td>
</tr>
<tr>
<td>Some application systems do not meet the password standards specified in P&amp;P</td>
</tr>
<tr>
<td>Some application systems have numerous users with &quot;super user&quot; status which allows elevated access rights</td>
</tr>
</tbody>
</table>
### Example Audit Findings

#### Business Continuity

- Close proximity of nuclear medicine to the computer room may restrict access to the computer room if a health-threatening nuclear medicine system failure occurs.

- Close proximity to the interstate and railroad may cause evacuation of a facility if a health-threatening spill occurs.

- Computer room is located on the basement level resulting in a higher chance of water damage from leaks and flooding.

- Not all servers housing ePHI are located in the secure computer room (i.e., some are located in departments).
WHAT YOU SHOULD BE DOING
What You Should Be Doing

- Review this presentation and share with other stakeholders
- Create an up-to-date inventory of where PHI and ePHI are received, used, stored and transmitted
- Perform a security risk analysis that meets OCR guidelines and develop a plan to mitigate risks
- Develop a security risk management program
- Review OCR HIPAA/HITECH audit protocol
- Perform a HIPAA/HITECH compliance gap analysis and develop a plan to mitigate gaps
- Develop a process to assess compliance throughout the year
QUESTIONS AND COMMENTS?
Lessons Learned from HIPAA Audits

October 29, 2012

Tony Brooks, CISA, CRISC
Partner - IT Assurance and Risk Services
HORNE LLP

tony.brooks@horne-llp.com