HIPAA Security Compliance Reviews

Elizabeth S. Holland, MPA
Office of E-Health Standards and Services
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
What is HIPAA?

- Administrative Simplification
  - Transactions and Codes Sets
  - Unique Identifiers
  - Security
  - Privacy
Covered Entities under HIPAA

- The Administrative Simplification standards adopted by HHS under HIPAA apply to any entity that is:
  - a health care provider that conducts certain transactions in electronic form
  - a health care clearinghouse, or
  - a health plan
Role of CMS/OESS

- OESS is responsible for
  - E-Health including e-prescribing, personal health records, Recovery Act coordination re: electronic health record incentives
- HIPAA:
  - Regulatory/Policy Interpretation (5010 and ICD-10)
  - Outreach and Education
  - Enforcement
HIPAA Security Rule

• Security Standards for the protection of Electronic Protected Health Information (ePHI)
• Applies to ePHI that a covered entity creates, receives, maintains, or transmits
• Published February 20, 2003
• Compliance Date April 20, 2005 (April 20, 2006 for small health plans)
HIPAA Security Rule – Security Standards

- Three categories of safeguards:
  - Administrative
  - Physical
  - Technical
HIPAA Enforcement

- Secretary of HHS delegated to the Administrator of CMS the authority to investigate complaints of non-compliance with HIPAA regulations
- Office for Civil Rights (OCR), HHS has responsibility for privacy
- Enforcement efforts are complaint based
CMS Enforcement Statistics Report
Open and Closed Cases by Type
As of April 30, 2009

<table>
<thead>
<tr>
<th>Complaint Type</th>
<th>Total</th>
<th>Open</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions and Code Sets (TCS)</td>
<td>614</td>
<td>43</td>
<td>571</td>
</tr>
<tr>
<td>Security</td>
<td>415</td>
<td>74</td>
<td>341</td>
</tr>
<tr>
<td>National Provider Identifier (NPI)</td>
<td>43</td>
<td>4</td>
<td>39</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1,072</td>
<td>121</td>
<td>951</td>
</tr>
</tbody>
</table>

**Open** – Outstanding issues remain. Entity may be under a corrective action plan or additional information from either the complainant, the filed against entity, or both is being sought.

**Closed** – No further action required. All issues have been sufficiently resolved. Please note that 47 of the 341 security cases have been closed via corrective action plans.
## Most Common Complaints

<table>
<thead>
<tr>
<th>Security Rule Section</th>
<th>Security Type Description</th>
<th>Number of complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(a)(4)(i)</td>
<td>Information Access Management</td>
<td>159</td>
</tr>
<tr>
<td>164.312(a)(1)</td>
<td>Access Control</td>
<td>158</td>
</tr>
<tr>
<td>164.308(a)(5)(i)</td>
<td>Security Awareness and Training</td>
<td>127</td>
</tr>
<tr>
<td>164.308(a)(6)(i)</td>
<td>Security Incident Procedures</td>
<td>103</td>
</tr>
<tr>
<td>164.310(d)(1)</td>
<td>Device and Media Control</td>
<td>73</td>
</tr>
</tbody>
</table>
HIPAA Security Compliance

• Expanded our work to build voluntary HIPAA compliance
• Began to conduct compliance reviews on covered entities
• Contracted with Price Waterhouse Coopers (PWC) for 10 reviews in 2008
HIPAA Security Compliance

• Selection of entities:
  • Entities against whom a complaint has been filed
  • Media reports of potential security violations

• Reviews focused:
  • on the allegations in the complaint or
  • Information in the media report
  • how the covered entity resolved the issues
HIPAA Security Compliance

• Issues included:
  • Risk analysis and management
  • Security training;
  • Physical security of facilities and mobile devices;
  • Off-site access and use of ePHI from remote locations;
  • Storage of ePHI on portable devices and media;
  • Disposal of equipment containing ePHI;
  • Business associate agreements and contracts;
  • Data encryption;
  • Virus protection;
  • Technical safeguards in place to protect ePHI; and
  • Monitoring of access to ePHI.
• Reviews were conducted in New York, Florida, California, Oregon, New Hampshire, North Carolina, Pennsylvania, Maryland
• Nine were of providers and one was a health plan
• Seven were hospitals, one pharmacy, and one home care/hospice provider
• Compliance reviews revealed areas where covered entities appeared to struggle:
  • Risk assessment
  • Currency of Policies and Procedures
  • Security Training
  • Workforce Clearance
  • Workstation Security
  • Encryption
HIPAA Security Compliance Reviews-2008

• Prepared Report: HIPAA Compliance Review Analysis and Summary of Results-2008 Reviews

• Outlines the six overarching compliance issues and provides recommended solutions as a guide to help improve compliance
HIPAA Security Compliance Reviews-2008

- Posted Compliance Review Examples
  - Related to Loss of Portable Device
  - Related to Theft of Backup Tapes
  - Related to Theft of Workstation and Backup Hard Drive
  - Related to Theft of Laptop
  - Related to a Computer Virus Infection
  - Related to Theft of Workstation and Backup Hard Drive
HIPAA Security Compliance Reviews

• Reviews have resulted in Corrective Action Plans (CAPs) that include:
  • Policies and procedures for remote use/access
  • Designation of internal security audit personnel
• CAPs are monitored by CMS
• Compliance review cases are generally closed when CMS verifies completion of CAP.
HIPAA Security Compliance Reviews-2009

- Contracted with Quality Software Services, Inc (QSSI) to do compliance reviews in 2009
- Six have been conducted or scheduled
- Not complaint based reviews
- Selected by covered entity type and location
HIPAA Security Compliance Reviews-2009

- Reviews in Florida, California, New York, Illinois, Minnesota, and Washington
- Three health plans, one clearinghouse, two providers (one federally qualified health center and one skilled nursing facility)
• Reviews are not meant to be punitive
• Improve compliance
  • Determine things that the entity is doing well (possible best practices that can be shared)
  • Determine areas where the covered entity can improve their compliance
HIPAA Security Compliance Reviews-2009

• Contact covered entity via letter sent by certified mail
  • Propose review dates
  • Propose date for pre-entrance conference call with CMS, QSSI and covered entity
• Request working space with electricity, phone with outside access and internet connectivity for at least five business days
HIPAA Security Compliance Reviews-2009

- Request documents
- Receive documents on a flow-basis
- Assess documents for compliance with the HIPAA regulations
- Periodic pre-review conference calls
- Formulate questions based on review of policies and procedures
HIPAA Security Compliance
Reviews-2009

• On-site review:
  • Interview staff
  • Review additional documentation
  • Review technical controls
  • Review results of past reviews and audits
• Draft report
• Final report of findings
• Creation of corrective action plans, if needed
HIPAA Security Compliance Reviews-2009-Interviews

- Director of Covered Entity (CE) organization under review.
- VP IT Security and Compliance
- SVP, Chief Compliance Officer
- VP Infrastructure
- IT Security Manager
- Direct Line Supervisor of individual or area where breach/incident occurred.
- Developer Executing the File Transfer During the Security Incident
HIPAA Security Compliance Reviews-2009-Interviews

- Lead systems manager or director.
- Systems security officer
- Computer Hardware specialist.
- Disaster recovery specialist or person in charge of backup tapes.
- Facility access control coordinator (physical security).
• Lead network engineer.
  • Individuals responsible for administration of platforms that store, transmit, or process ePHI.
  • Individuals responsible for administration of the site network (wired and wireless).
  • Individuals responsible for monitoring of platforms that store, transmit, or process ePHI.
  • Individuals responsible for monitoring the network (if different from above).
HIPAA Security Compliance Reviews-2009-Interviews

- Human resources representative.
- Director of training.
- Individual responsible for policy and procedure management
- Incident response team leader.
- Access to all members of workforce.
• All policies and procedures designed to demonstrate compliance with the HIPAA Security Rule Administrative Safeguards mapped to the specific HIPAA Security Administrative Safeguard.
• Policies and procedures to prevent, detect, contain, and correct security violations.
• Policies and procedures address setting up a user’s access profile.
• Policies and procedures that address detecting, reporting, and responding to security incidents (if not in the security plan).
• Physical security policies.
HIPAA Security Compliance Reviews-2009-Sample Request

- Policies and procedures that address encryption and decryption of electronic PHI.
- Policies and procedures that address mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives).
- Policies outlining the entity's monitoring of system usage - authorized and unauthorized attempts.
- Policies regarding the use of wireless networks in the environment.
• Templates and/or documents used to record the acknowledgement of use of wireless networks, mobile computing, as well as remote access to systems.
• Periodic vulnerability scanning policy and procedure.
• Periodic network penetration testing policy and procedure.
• Access to security violation monitoring reports.
• Security violation monitoring reports templates.
HIPAA Security Compliance Reviews-2009-Sample Request

- Access to reports developed related to follow up action taken from violations that have occurred.
- **Security violation follow-up action log/report templates.**
- Policies and procedures that address granting, approving, and monitoring emergency access IDs during an emergency situation.
- Policies and procedures that outline hiring and termination procedures.
- Policies related to employee background checks and confidentiality agreements.
• Templates and/or documents used to record the processing of background checks and confidentiality agreements.
• Policies related to periodic reviews of appropriateness for personnel with access to PHI.
• Policies for granting system access (for example, by level, role, and job function.
• Policies and procedures that address creating, changing, and safeguarding passwords.
• Templates and/or documents used to record the creating, changing, and safeguarding passwords.
• Policies related to the timely removal of personnel from the system environment.
• Policies and procedures regarding secure workstation use are documented and address specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage).
• Policies and procedures that address the secure disposal of hardware, software, and the electronic PHI data.
• Templates and/or documentation used to record the secure disposal of hardware, software, and the electronic PHI data.
• Most recent high-level risk assessment. Review risk assessment policies.
• Risk assessment template documentation
• Other documents: http://www.cms.hhs.gov/Enforcement/09_HIPAAComplianceReviewInformationandExamples.asp
• Vulnerabilities identified:
  • HIPAA Security Policies and Procedures
  • Business Associate Agreements
  • Encryption of ePHI on mobile devices
  • HIPAA Security Training
HIPAA Compliance

- Looking to the future – continuation a three-pronged approach:
  - Complaint management
  - Compliance reviews
  - Outreach and Education