OCR Reports on the Enforcement of the HIPAA Rules

HCCA Compliance Institute
April 22, 2013
David Holtzman
Sr. Health IT & Privacy Specialist

U.S. Department of Health and Human Services
Office for Civil Rights

Learning Objectives

1. Update on OCR’s enforcement of Privacy/Security/Breach Notification Rules

2. Discuss the practical implications of the final breach notification rule and enforcement rule

3. Learn about HHS tools you can use in your privacy and security awareness training
### HIPAA Compliance/Enforcement
(As of December 31, 2012)

<table>
<thead>
<tr>
<th>TOTAL (since 2003)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Filed</td>
<td>77,200</td>
</tr>
<tr>
<td>Cases Investigated</td>
<td>27,500</td>
</tr>
<tr>
<td>Cases with Corrective Action</td>
<td>18,600</td>
</tr>
<tr>
<td>Civil Monetary Penalties &amp; Resolution Agreements (since 2008)</td>
<td>$14.9 million</td>
</tr>
</tbody>
</table>

### Issues Most Frequently Reviewed

<table>
<thead>
<tr>
<th>Privacy Rule</th>
<th>Security Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impermissible Uses and Disclosures of PHI</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Safeguards to Protect Health Information</td>
<td>Security Incident Response and Reporting</td>
</tr>
<tr>
<td>Access to Health Records</td>
<td>Security Awareness and Training</td>
</tr>
<tr>
<td>Minimum Necessary</td>
<td>Access Controls</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>Encryption and Decryption (Data in Storage)</td>
</tr>
</tbody>
</table>
Breach Notification Highlights
September 2009 through March 20, 2013

• 556 reports involving over 500 individuals
• Over 78,000 reports involving under 500 individuals
• Top types of large breaches
  – Theft
  – Unauthorized Access/Disclosure
  – Loss
• Top locations for large breaches
  – Laptops
  – Paper records
  – Desktop Computers
  – Portable Electronic Device

Spotlight on Largest Breaches of 2012

• Hacking network server – 780,000 affected
• Backup tapes stored at hospital cannot be found and are presumed lost – 315,000 affected
• Unencrypted emails sent to employee’s unsecured email address -- 228,435 affected
• Theft of laptop from employee’s vehicle – 116,506 affected
• Unauthorized access to e-PHI stored in database-- 105,646 affected
• Hacking database stored on network server – 70,000 affected
Breach Notification:
500+ Breaches by Type of Breach

Unauthorized Access/ Disclosure 20%

Unauthorized Access/ Disclosure 20%

Theft 52%

Loss 13%

Improper Disposal 5%

Improper Disposal 5%

Hacking/IT Incident 8%

Hacking/IT Incident 8%

Unauthorized Access/ Disclosure 20%

Breach Notification:
500+ Breaches by Location of Breach

Laptop 23%

Desktop Computer 15%

EMR 2%

EMR 2%

Network Server 11%

Network Server 11%

E-mail 2%

E-mail 2%
Major 2012 Enforcement Actions

• BCBS Tennessee ($1.5 M)
  – E-PHI stored on servers stolen from deactivated data center after construction/relocation to new facility
  – Reevaluate threats/vulnerabilities to e-PHI caused by changing operational environment and manage risk

• Phoenix Cardiac Surgery ($100K)
  – E-PHI disclosed through Internet when provider used third party application hosted in the cloud
  – Business associate agreements required when sharing data with cloud computing service providers

• Alaska DHSS ($1.7M)
  – Portable storage device stolen from personal vehicle symptomatic of widespread failure to implement program-wide information security safeguards
  – Risk analysis to identify location and safeguards for PHI, training and controls for portal devices

U.S. Department of Health and Human Services, Office for Civil Rights

4/1/2013

Major Enforcement Actions of 2012

• Massachusetts Eye and Ear Institute ($1.5M)
  – Stolen personal laptop of physician using device as desktop substitute
  – Covered entity had not implemented a program to mitigate identified risks to e-PHI
  – Encrypt data stored on end-user devices

• Hospice of Northern Idaho ($50K)
  – Breach affecting 400 individuals when laptop stolen
  – Provider had not conducted a risk assessment or taken other measures to safeguard e-PHI as required by Security Rule
  – Implement security measures to safeguard e-PHI

U.S. Department of Health and Human Services, Office for Civil Rights
April 22, 2013 | page 10
Audit Program

• HITECH Act – Sec. 13411
  – Periodic audits to ensure covered entities and business associates comply with requirements of HIPAA and HITECH

• Audit Objectives
  – Examine mechanisms for compliance
  – Identify best practices
  – Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  – Renew attention of covered entities to health information privacy and security compliance activities

Audit Pilot Completed

• Pilot Process
  – Tiered approach for snapshot of compliance across covered entity types, sizes, complexity
  – Sample of 115 covered entities selected spread across 4 tiers
  – All audits completed by December 2012
  – Published audit protocol
  – Issuing final reports to 115 entities audited in pilot and assessing findings

• Conducting Evaluation of Audit Pilot
Audit Pilot Observations

• Completed Audits of 115 entities
  - 61 Providers, 47 Health Plans, 7 Clearinghouses
• No findings or observations for 13 entities (11%)
  - 2 Providers, 9 Health Plans, 2 Clearinghouses
• Total 979 audit findings and observations
  - 293 Privacy
  - 592 Security
  - 94 Breach Notification
• Percentage of Security Rule findings and observations was double what would have been expected based on protocol
• Smaller entities (Level 4) struggle with all three areas

Omnibus Final Rule – Important Dates

• Public Display at Federal Register – January 17, 2013
• Published in Federal Register – January 25, 2013
• Effective Date – March 26, 2013
• Compliance Date – September 23, 2013
• Conform BA contracts – September 22, 2014
Omnibus Final Rule – What’s New for Business Associates

• BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule
  – Liable for Security Rule violations
• BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule
  – Criminal and civil liabilities for violations
• BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
• Subcontractors of a BA are now defined as a BA
  – BA liability flows to all subcontractors

Omnibus Final Rule – What’s New for Breach

• Breach Notification Provisions
  – Replaces “harm to individual” with more objective measure of compromise to the data as threshold for breach notification
  – Other provisions of 2009 IFR adopted without major change
Omnibus Final Rule – What’s New for Enforcement

- Enforcement Provisions
  - Adopts increased CMP amounts and tiered levels of culpability from 2009 IFR
  - Clarifies “Reasonable Cause” Tier
  - Willful Neglect Penalties do not require informal resolution
  - Intentional wrongful disclosures may be subject to civil, rather than criminal, penalties

HITECH Enforcement Raises CMP Levels

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Identical Violations per Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Enforcement Rule: Investigation and Resolution of Violations

The Final Rule reflects the requirement of the HITECH Act that HHS will investigate a possible HIPAA violation if a preliminary review of the facts available from a complaint or a compliance review, or information from an independent inquiry by HHS, indicates the possibility of willful neglect.

- The investigation may proceed directly to an enforcement action, particularly but not only, in the case of willful neglect.
- However, the Final Rule offers reassurance that, absent indications of willful neglect, HHS still will seek compliance through informal, voluntary action in appropriate cases.

Enforcement Rule: Violations Due to Reasonable Cause

Of the four tiers of penalties specified in the HITECH Act, the required state of mind for the “lowest” tier (entity did not know, and in the exercise of reasonable diligence would not have known of the violation) and for the “highest” two tiers (willful neglect) are unchanged under the Final Rule.

- The state of mind for second tier, violations due to reasonable cause not amounting to willful neglect, was not specified in the HITECH Act.
Enforcement Rule: Violations Due to Reasonable Cause

• The second tier is important as a practical matter, because it likely covers many common violations by otherwise generally compliant covered entities and business associates, such as those that occur due to human error, despite workforce training and appropriate policies and procedures.

• Modifies the definition of reasonable cause to specify the state of mind; reasonable cause covers violations in which the entity exercised ordinary business care and prudence to comply with the provision that was violated or in which the entity knew of the violation but lacked “conscious intent or reckless indifference” associated with a violation due to willful neglect.

HIPAA: Creating Awareness and Educating Providers on the Importance of Compliance

Medscape: Free CME and CE Training

ONC/OCR Mobile Device Program
Instructional Video Series

The videos explore mobile device risks and discuss privacy and security safeguards providers and professionals can put into place to mitigate risks.

Securing Your Mobile Device is Important!

Dr. Anderson's Office Identifies a Risk

A Mobile Device is Stolen

Protecting Patients' Health Information When Using a Public Wi-Fi Network?

Worried About Using a Mobile Device for Work? Here's What To Do!

Downloadable Materials
www.healthit.gov/mobiledevices

• Fact sheets
• Posters
• Brochures
Guidance/Compliance Tools

- De-identification Guidance
- Sample Business Associate Contract Language
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- Risk Analysis Guidance
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/rafinalguidance.html
- Security for Mobile Devices (video/web)
  http://www.healthit.gov/mobiledevices

Questions?

OCR website  www.HHS.gov/OCR/Privacy

Contact Information  david.holtzman@hhs.gov