Keeping Health Information Private and Secure

New Initiatives and Tools

Office of the National Coordinator

December 12, 2012
HITECH Regulations and Enforcement

Director Leon Rodriguez
U.S. Department of Health and Human Services
Office for Civil Rights
Breach Notification Reports

• Universe of breach notification reports
  – Over 500 reports involving 500 or more individuals, +21.4 million individuals affected and growing
  – 3,684,514 individuals affected by theft or loss of laptops or other portable electronic devices
  – Over 60,500 reports involving under 500 individuals

• Top types of large breaches
  – Theft
  – Unauthorized Access/Disclosure
  – Loss

• Top locations for large breaches
  – Paper records
  – Laptops
  – Desktop Computers
  – Portable Electronic Device
Breach Notification
500+ Breaches by Type of Breach

Unauthorized Access/Disclosure: 21%
Theft: 51%
Loss: 13%
Hacking/IT Incident: 7%
Improper Disposal: 5%
Unknown: 3%

Data as of October 3, 2012
Breach Notification
500+ Breaches by Location of Breach

Data as of October 3, 2012
Breach Notification Reports

Recent Breaches and Highlights

• Hacking incident involving network server (780,000 affected)
• Backup tapes stored at hospital cannot be found (315,000 affected)
• Unencrypted emails sent to employee’s unsecured email address (228,435 affected)
• Theft of electronic medical records from covered entity (102,153 affected)
• Theft of laptop from contractor’s vehicle (66,601 affected)
• Unauthorized disclosure of protected health information (PHI) by employees (64,846 affected)
• Theft of portable electronic device from employee’s vehicle (55,000 affected)

Data as of October 3, 2012
### Breakdown of First 20 Auditees

<table>
<thead>
<tr>
<th>Level 1 Entities - <em>Large provider / health plan</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 11% of the first 20 auditees</td>
</tr>
<tr>
<td>• 4% with privacy audit issues</td>
</tr>
<tr>
<td>• Extensive use of HIT - complicated HIT enabled clinical /business work streams</td>
</tr>
<tr>
<td>• Revenues and or assets greater than $1 billion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 2 Entities - <em>Large regional hospital system (3-10 hospitals/region) / regional insurance company</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 8% of the first 20 auditees</td>
</tr>
<tr>
<td>• 3% with privacy audit issues</td>
</tr>
<tr>
<td>• Paper and HIT enabled work flows</td>
</tr>
<tr>
<td>• Revenues and or assets between $300 million and $1 billion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 3 Entities - <em>Community hospitals, outpatient surgery, regional pharmacy / self-insured entities that do not adjudicate their claims</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 15% of the first 20 auditees</td>
</tr>
<tr>
<td>• 16% with privacy audit issues</td>
</tr>
<tr>
<td>• Some but not extensive use of HIT – mostly paper based workflows</td>
</tr>
<tr>
<td>• Revenues between $50 - $300 million</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 4 Entities - <em>Small providers (10 to 50 provider practices, community or rural pharmacy)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 66% of the first 20 auditees</td>
</tr>
<tr>
<td>• 77% with privacy audit issues</td>
</tr>
<tr>
<td>• Little to no use of HIT – almost exclusively paper based workflows</td>
</tr>
<tr>
<td>• Revenues less than $50 million</td>
</tr>
</tbody>
</table>
Initial 20 Findings Analysis
Overview

Analysis of Findings by Rules

- Security: 65%
- Privacy: 26%
- Breach: 9%
Initial 20 Findings Analysis

Overview

Analysis by Type of Covered Entity

Data as of June 2012
Initial 20 Findings Analysis
Overview

Analysis of Finding by Tier

Data as of June 2012
Initial 20 Findings Analysis
Privacy: Uses and Disclosures

Uses and Disclosures Analysis

Data as of June 2012
Initial 20 Findings Analysis Privacy: Notice and Access

Notice of Privacy Practices for PHI – §164.520

Data as of June 2012.

U.S. Department of Health and Human Services, Office for Civil Rights
Initial 20 Findings Analysis
Privacy: Administrative Requirements

Administrative Requirements – §164.530

Data as of June 2012.
Initial 20 Findings Analysis
Security Issues

Security Audit Issues by Type of Entity

Data as of June 2012.
Initial 20 Findings Analysis Security Issues

Security Audit Issues by Level of Entity

Data as of June 2012.

U.S. Department of Health and Human Services, Office for Civil Rights
Initial 20 Findings Analysis
Security Issues

Security Audit Issues by Area of HIPAA
Security Rule

- Administrative Safeguards – §164.308: 42.70%
- Physical Safeguards – §164.310: 16.76%
- Technical Safeguards – §164.312: 40.54%

Data as of June 2012.

U.S. Department of Health and Human Services, Office for Civil Rights
Initial 20 Findings Analysis
Security Top Issues

Data as of June 2012.
Initial 20 Findings
Preliminary Observations

• Policies and procedures
• Priority HIPAA compliance programs
• Small providers
• Larger entities security challenges
• Conduct of risk assessments
• Managing third party risks
• Privacy challenges widely dispersed throughout protocol
• No clear trends by entity type or size
## HIPAA Compliance and Enforcement

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Amount</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Massachusetts Eye and Ear Infirmary</td>
<td>$1.5 Million</td>
<td>September 17, 2012</td>
</tr>
<tr>
<td>Alaska Department of Health and Social Services</td>
<td>$1.7 Million</td>
<td>June 26, 2012</td>
</tr>
<tr>
<td>Phoenix Cardiac Surgery</td>
<td>$100,000</td>
<td>April 13, 2012</td>
</tr>
<tr>
<td>Blue Cross Blue Shield of Tennessee</td>
<td>$1.5 Million</td>
<td>March 13, 2012</td>
</tr>
<tr>
<td>University of California at Los Angeles Health System</td>
<td>$865,500</td>
<td>July 6, 2011</td>
</tr>
<tr>
<td>Massachusetts General Hospital</td>
<td>$1 Million</td>
<td>February 14, 2011</td>
</tr>
<tr>
<td>Cignet Health of Prince George's County, MD (Civil Money Penalty)</td>
<td>$4.3 Million</td>
<td>February 4, 2011 (August 28, 2012)</td>
</tr>
<tr>
<td>Management Services Organization of Washington, Inc.</td>
<td>$35,000</td>
<td>December 13, 2010</td>
</tr>
<tr>
<td>Rite Aid Corporation</td>
<td>$1 Million</td>
<td>July 27, 2010</td>
</tr>
<tr>
<td>CVS Pharmacy, Inc.</td>
<td>$2.25 Million</td>
<td>January 16, 2009</td>
</tr>
<tr>
<td>Providence Health &amp; Services</td>
<td>$100,000</td>
<td>July 16, 2008</td>
</tr>
</tbody>
</table>

**Total Complaints filed (since 2003): 74,554**

Data as of December 31, 2011.

**Total Cases Investigated: 26,513**

**Total Cases with Corrective Action: 17,767**
### HIPAA Compliance and Enforcement

**Issues and Results (2008 – present)**

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Issue</th>
<th>Results of OCR Investigation</th>
</tr>
</thead>
</table>
| + Massachusetts Eye and Ear Infirmary (MEEI)  
   September 17, 2012  
   $1.5 Million | Breach report submitted by MEEI reporting the theft of an unencrypted personal laptop containing electronic protected health information (ePHI) of MEEI patients and research subjects. | • Failure to conduct a risk analysis.  
• Failure to implement security measures for portable devices.  
• Failure to implement policies and procedures to restrict access to ePHI.  
• Failure to implement policies and procedures regarding security incident identification, reporting, and response. |
| + Alaska Department of Health and Social Services (DHSS)  
   June 26, 2012  
   $1.7 Million | Breach report submitted by Alaska DHSS indicating that a portable electronic storage device (USB hard drive) possibly containing electronic protected health information (ePHI) was stolen from the vehicle of an Alaska DHSS employee. | • Failure to complete a risk analysis.  
• Failure to implement risk management measures.  
• Failure to complete security training.  
• Failure to implement device and media controls.  
• Failure to address device and media encryption. |
| Phoenix Cardiac Surgery  
   April 13, 2012  
   $100,000 | • Physician practice posted clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible.  
• Implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules.  
• Limited safeguards in place to protect patients’ electronic protected health information (ePHI). | • Failure to implement adequate policies and procedures.  
• Failure to document training.  
• Failure to identify a security official and conduct a risk analysis.  
• Failure to obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI. |

+ = OCR resolution agreements resulting from investigations initiated after a covered entity's reporting of a breach incident.

* = Findings of noncompliance were made in a Notice of Proposed Determination on October 25, 2010.
<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Issue</th>
<th>Results of OCR Investigation</th>
</tr>
</thead>
</table>
| + Blue Cross Blue Shield of Tennessee (BCBST)  
March 13, 2012  
$1.5 Million | Breach notice submitted by BCBS  
Tennessee to HHS in which it was  
reported that 57 unencrypted computer  
hard drives containing protected health  
information (PHI) of over 1 million  
individuals had been stolen from a leased  
facility in Tennessee. | • Failure to implement appropriate administrative safeguards.  
• Failure to perform the required security evaluation following operational changes.  
• Failure to implement appropriate facility access controls. |
| University of California at Los Angeles Health System (UCLA HS)  
July 6, 2011  
$865,500 | Unauthorized employees repeatedly looked at the electronic protected health information (ePHI) of numerous UCLA HS patients. | • Failure to conduct Privacy and Security trainings.  
• Did not implement sanctions policy.  
• Failure to implement security measures to reduce the risks of impermissible access to ePHI. |
| Massachusetts General Hospital  
February 14, 2011  
$1 Million | Loss of protected health information (PHI) of 192 patients of Mass General’s Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. | • Impermissible disclosure of PHI.  
• Failure to implement safeguards to protect PHI when removed from Massachusetts General’s premises. |
| * Cignet Health of Prince George’s County, MD (Cignet)  
(Civil Money Penalty)  
February 4, 2011  
$4.3 Million | Violated the right to access medical records of 41 patients. | • Failure to provide copies of the patient’s records.  
• Failure to respond to OCR’s investigation. |

+ = OCR resolution agreements resulting from investigations initiated after a covered entity's reporting of a breach incident.  
* = Findings of noncompliance were made in a Notice of Proposed Determination on October 25, 2010.
## HIPAA Compliance and Enforcement

### Issues and Results (2008 – present), continued

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Issue</th>
<th>Results of OCR Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Services Organization of Washington</td>
<td>Disclosure of electronic protected health information for marketing purposes.</td>
<td>Did not have in place or implement appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of the protected health information.</td>
</tr>
<tr>
<td>December 13, 2010</td>
<td>$35,000</td>
<td></td>
</tr>
</tbody>
</table>
| Rite Aid Corporation                                | Protected health information (PHI) disposed of in dumpsters that were not secure and could be accessed by the public. | - Failure to implement adequate policies and procedures to safeguard PHI during the disposal process.  
- Failure to adequately train employees on the disposal process.  
- Did not maintain and implement a workforce sanctions policy. |
| July 27, 2010                                       | $1 Million                                                            |                                                                                                |
| CVS Pharmacy, Inc.                                  | Protected health information (PHI) disposed of in dumpsters that were not secure and could be accessed by the public. | - Failure to implement adequate policies and procedures to safeguard PHI during the disposal process.  
- Failure to adequately train employees on the disposal process.  
- Did not maintain and implement a workforce sanctions policy. |
| January 16, 2009                                    | $2.25 Million                                                         |                                                                                                |
| Providence Health & Services                        | Loss and theft of electronic backup media and laptop computers containing individually identifiable health information. | Failure to implement policies and procedures to safeguard individually identifiable health information. |
| July 16, 2008                                       | $100,000                                                              |                                                                                                |

+ = OCR resolution agreements resulting from investigations initiated after a covered entity's reporting of a breach incident.  
* = Findings of noncompliance were made in a Notice of Proposed Determination on October 25, 2010.
Consumer Videos

Visit the HHS OCR youtube channel at [youtube.com/user/USGovHHSOCR](http://youtube.com/user/USGovHHSOCR) or our website at [HHS.gov/OCR](http://HHS.gov/OCR)
Keeping Health Information Private and Secure
Snapshot of OCPO’s Research & Internal Initiatives

• Data Segmentation for Privacy Initiative
  – Demonstration Planned 1st Q 2013
• eConsent Trial Project
  – Pilot launched in October 2012
• SHARPS Grants on Privacy and Security Innovations
• Patients’ Attitudes toward Privacy and Security Survey
• Notice of Privacy Practices (NPP) Project
• Provider and Staff Security Video Games
• Mobile Device Portfolio
  – mHealth Consumer/Patient Research
  – Mobile Device Provider Education
Mobile Devices:
Know the RISKS. Take the STEPS.
PROTECT and SECURE
Health Information.

Learn more at HealthIT.gov/mobiledevices
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

Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?

Worried About Using a Mobile Device for Work? Here's What To Do!
Online Resource Center:
Tips to Protect and Secure Health Information

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate wiping and/or remote disabling.
- Disable and do not install file-sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep security software up to date.
- Research mobile applications (apps) before downloading.
- Maintain physical control of your mobile device.
- Use adequate security to send or receive health information over public Wi-Fi networks.
- Delete all stored health information before discarding or reusing the mobile device.
Easy to Download Resources

- Fact sheets
- Posters
- Brochure

Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT & SECURE Health Information.

Find out more at HealthIT.gov/mobiledevices

10 tips to protect and secure health information when using a mobile device.

1. Use a password or other user authentication
2. Install and enable encryption
3. Install and activate remote wiping or remote disabling
4. Do not install or use file sharing applications
5. Install and enable a firewall
6. Keep security software and keep it up to date
7. Research mobile applications before downloading
8. Always keep your device in your possession
9. Use adequate security to send or receive health information over public Wi-Fi networks
10. Delete all stored health information before discarding the mobile device

Be a team player.
Understand and follow your organization’s mobile device policy and procedures.
It’s your responsibility.
Visit HealthIT.gov/mobiledevices
Mobile Devices: **Know the RISKS. Take the STEPS.**

**PROTECT & SECURE** Health Information

Find out more at HealthIT.gov/mobiledevices
Privacy & Security References


• Data Segmentation for Privacy Initiative: [http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage](http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage)


• Provider and Staff Security Video Game: [http://www.healthit.gov/providers-professionals/privacy-security-training-games](http://www.healthit.gov/providers-professionals/privacy-security-training-games)

• Mobile Device Privacy & Security Resource Center: [www.healthit.gov/mobiledevices](http://www.healthit.gov/mobiledevices)

