Security Lessons Learned from HIPAA Enforcement

Presentation to HealthSec ‘12
August 7, 2012

Adam H. Greene, J.D., M.P.H.
Partner, Davis Wright Tremaine
Enforcement of the Security Rule

- Initially enforced by HHS Centers for Medicare & Medicaid Services (CMS)
- HHS Office for Civil Rights (OCR) took over enforcement in July 2009
1. Lack of information access management
2. Lack of access controls
3. Lack of security awareness and training
4. Lack of security incident response and reporting
5. Lack of device and media controls
Top Security Issues (2011)

1. Lack of risk analysis
2. Lack of security incident response and reporting
3. Lack of security awareness and training
4. Lack of access controls
5. Failure to address encryption and decryption (data in storage)
Overview of Breach Reports

- 452 large breaches reported between Sept. 2009 and June 2012
- Over 50,000 small breaches reported in same period
- Over 20 million individuals affected by large breaches
Lesson 1:

You should be less concerned with:

And more concerned with:
Causes of Large Breaches (by number of breaches)
Sept. 2009 to June 2012

- Theft, 234, 52%
- Loss, 59, 13%
- Unauthorized Access/Disclosure, 93, 21%
- Hacking/IT Incident, 31, 7%
- Improper Disposal, 24, 5%
- Unknown, 7, 1%
- Other, 3, 1%

Unauthorized Access/Disclosure, 93, 21%
Cause of Large Breach (by # of affected individuals)  
Sept. 2009 to June 2012

- **Theft**, 7,924,146, 38%
- **Unauthorized Access/Disclosure**, 7,314,610, 35%
- **Loss**, 2,226,160, 11%
- **Improper Disposal**, 1,230,299, 6%
- **Hacking/IT Incident**, 1,565,300, 7%
- **Unknown**, 350,961, 2%
- **Other**, 156,398, 1%
Lesson 2:

The highest number of breaches involve:

a) Desktops
b) Laptops
c) Other portable devices
d) Paper
Location of Large Breaches (by # of breaches)
Sept. 2009 to June 2012

- Paper, 114, 25%
- Laptop, 104, 23%
- Other Portable Electronic Device, 65, 14%
- Computer, 61, 14%
- Network Server, 47, 10%
- Other, 36, 8%
- Electronic Medical Record, 8, 2%
- E-mail, 11, 3%
- Other (Backup Tapes), 5, 1%
- Other (hard drives), 1, 0%
Location of Large Breach (# of individuals affected) Sept. 2009 to June 2012

- **Other (Backup Tapes)**, 6,284,483, 30%
- **Other**, 3,799,900, 18%
- **Network Server**, 2,393,017, 12%
- **Computer**, 2,290,566, 11%
- **Laptop**, 1,938,235, 9%
- **Electronic Medical Record**, 1,146,335, 6%
- **Other (hard drives)**, 1,023,209, 5%
- **Other Portable Electronic Device**, 981,131, 5%
- **Paper**, 643,912, 3%
- **E-mail**, 267,172, 1%
Lesson 3:

It isn’t me, it’s you …

- Many large breaches are caused by business associates, not covered entities
Large Breaches Caused by BAs (by # of breaches)  
Sept. 2009 to June 2012

- Covered Entity, 356, 79%
- Business Associate, 96, 21%
Large Breaches (by # of affected individuals)  
Sept. 2009 to June 2012

- Covered Entity, 8,684,465, 42%
- Business Associate, 12,083,409, 58%
Privacy and Security Audits

- First substantial HIPAA privacy and security audits
- First proactive review (rather than incident driven)
- Audits include site visits and audit reports
- Includes very limited notice (10-15 business days to produce documents)
- Site visits of 3-5 persons for 3-10 days
### Who Will Be Audited: First 20 Audits

<table>
<thead>
<tr>
<th></th>
<th>Level 1&gt; $1B</th>
<th>Level 2 $300M - $1B</th>
<th>Level 3 $50M - $300M</th>
<th>Level 4 &lt;$50M</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Plans</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Health care providers</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Healthcare clearinghouses</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>6</td>
<td>3</td>
<td>6</td>
<td>20</td>
</tr>
</tbody>
</table>
Initial Audit Results

Analysis of Findings by Rules

- Security: 65%
- Privacy: 26%
- Breach: 9%

Source: “2012 HIPAA Privacy and Security Audits,” OCR/NIST Conference, 6/7/12
Initial Audit Results

Analysis by Type of Covered Entity

- 81% Provider
- 16% Health Plan
- 4% Clearinghouse

Source: “2012 HIPAA Privacy and Security Audits,” OCR/NIST Conference, 6/7/12
Initial Audit Results

Analysis of Finding by Tier

Source: “2012 HIPAA Privacy and Security Audits,” OCR/NIST Conference, 6/7/12
Initial Audit Results

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%

Source: “2012 HIPAA Privacy and Security Audits,” OCR/NIST Conference, 6/7/12
Initial Audit Results

Security Audit Issues by Area

- Conduct Risk Assessment: 17
- Grant, Modify User Access: 17
- Incident Response: 11
- Contingency Planning: 34
- Media Reuse and Destruction: 18
- Encryption: 10
- User Activity Monitoring: 46
- Authentication / Integrity: 19
- Physical Access Controls: 9

Source: “2012 HIPAA Privacy and Security Audits,” OCR/NIST Conference, 6/7/12
HHS Settlements/Penalties

- Issues that have led to HHS settlements*:
  - Breaches involving over 350,000 (Providence, BCBS of Tennessee)
  - Breaches involving sensitive information, such as HIV or celebrities (Mass General, UCLA)
  - Improper disposal “caught on tape” (CVS, Rite Aid)

* Settlements represent allegations not formal findings
HHS Settlements/Penalties

- Issues that have led to HHS settlements*:
  - Improper disclosure for marketing (discovered through OIG/DOJ false claims investigation) (MSO Washington)
  - Inappropriate use of online calendar/general lack of compliance, lack of BAs (Phoenix Cardiac Surgeons)

- Issue that has led to a penalty
  - Refusal to cooperate with OCR investigation (Cignet)

* Settlements represent allegations not formal findings
State AGs Join the Party

- HITECH Act (2009) provided State attorneys general authority to enforce HIPAA
  - Four suits have been brought (three settled) (CT, VT, MN, and MA)
  - None have coincided with HHS formal action
- Issue that has led to AG actions: Large breaches
  - Large breach can lead to multiple AG settlements and other enforcement
- Average settlement: $260,000

* Settlements represent allegations not formal findings
Hipaa Criminal Cases

- Almost 20 criminal convictions
  - Began mostly with financial fraud cases
  - More recent convictions involve snooping
- Mostly employees
- Penalties range from probation and community service to over a year imprisonment
Lessons Learned

- HHS and State AGs focus enforcement on breaches and headlines
  - Encrypt, encrypt, encrypt
  - Focus on large data sets, including back-up tapes and spreadsheets
  - Pay close attention to VIPs and sensitive information
Lessons Learned

- HHS tends to look for systematic problems
  - Was a breach due to systematic failures?
  - Were there policies? Training? Sanctions? Auditing?
- HHS has a history of voluntary enforcement, but settlements are increasing (a few a year)
For more information

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP
adamgreene@dwt.com
202.973.4213