In the Trenches:
OCR Audits, Data Breaches, and Cybersecurity Threats & Mitigations
Health Care Compliance Association
June 16, 2017
PRESENTED BY
Leann Habte
Partner, Best Best & Krieger
Darrell Contreras
Chief Compliance Officer, Millennium Health
Linh Sithihao
Information Security Consultant, Woodford Consulting Inc.

Enforcement
- Increasing Federal Enforcement
  - OCR Audits
  - OCR Investigations of HIPAA Complaints
  - OCR Breach Investigations
- State Enforcement Less Pronounced Recently

The Good News
- Audit
  - Phase II desk reviews conducted for 166 Covered Entities and 43 Business Associates
  - On-site reviews on hold for 2017
- Issues Identified in Audits
  - Poor controls over systems that maintain PHI
  - Mobile devices, including laptops, that are not properly protected
The Bad News

- Aggressive Enforcement Continuing by Office for Civil Rights (OCR)
  - $14+ million in fines/civil monetary penalties in 2017
  - Heightened fines expected going forward
  - Increased focus on security safeguards to protect against digital health threats, cyber threats

Trends – Types of Violations Fined

- Highest Fines in 2017

<table>
<thead>
<tr>
<th>Amount of Fine</th>
<th>Violations Cited</th>
<th>Number of Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2.2 Million</td>
<td>Impermissible disclosure to news media</td>
<td>1</td>
</tr>
<tr>
<td>$2.5 Million</td>
<td>Loss/theft + lack of risk analysis/risk management + lack of HIPAA policies</td>
<td>1,391</td>
</tr>
<tr>
<td>$5.5 Million</td>
<td>Lack of access/audit controls</td>
<td>115,143</td>
</tr>
<tr>
<td>$5.2 Million</td>
<td>Loss of blackberry and laptop + lack of risk analysis/risk management + lack of corrective action</td>
<td></td>
</tr>
<tr>
<td>$2.2 Million</td>
<td>Loss/theft of USB drive + lack of risk management</td>
<td>2,209</td>
</tr>
</tbody>
</table>

Trends - Types of Violations Cited

- Most Common Violations Cited – 12 months

- Loss/Theft
- Lack of Risk Analysis/Risk Management
- Lack of Encryption
- Impermissible Disclosures
- Lack of BAA
- Lack of Policies
OCR’s Wall of Shame - 2016

• Breach Type
  ▪ Hacking/IT
  ▪ Theft/Loss
  ▪ Impermissible Disclosures

• Further Analysis Shows:
  ▪ 30% of breaches reported involve third parties.
  ▪ 48% of total incidents reported were Insider Breaches.
    ▪ 52% - employee errors or accidents
    ▪ 48% - intentional wrong-doing by employees


California Office of Attorney General

• Health Care Sector Breaches
  ▪ The health care sector accounted for 16% of breaches (103) and 14 percent (6.8 million) of Californians’ records breached from 2012 - 2015.
  ▪ Significantly higher incidence of breaches resulting from physical theft and loss: 54 percent compared to just 16 percent in all other sectors. See figure 17.

• Health Care Sector vs. Others - Type of Breach

Future Guidance by OCR

• Text messaging
• Social media
• Security of Electronic Health Records
• The “minimum necessary” requirement

• Provide individuals harmed by HIPAA violations with a percentage of any civil monetary penalties or settlements collected by Office fo Civil Rights
Mitigation Strategies for the Current Enforcement Landscape

Summary of Recent Settlements

- Over $14M in 2017 so far!
- Memorial Healthcare System - $5.5M failure to terminate access rights and review system access logs (PHI stolen by employees)
- Children's Medical Center of Dallas - $3.2M for 1 lost BlackBerry and 1 stolen laptop
- CardioNet, Inc. - $2.5M for 1 laptop stolen from a car and no policies
- Memorial Hermann - $2.4M (privacy issue)
- (2016) Catholic Health Care Services of the Archdiocese of Philadelphia - $650,000 resulting from theft of mobile device with PHI and no risk management plan.

Data Breach Nuggets

2016 Report:
- The average health care breach cost: $358/record
- 48% of all breaches caused by malicious or criminal attacks

Look back approach:
- If breach, then which rule would have prevented it?
How to Mitigate the Risk

CONTENT:
- Security Assessment — Select a path for ePHI
  - How could ePHI leave the organization?
  - Where is our ePHI located?
  - How could someone gain access to the ePHI?

STRUCTURE:
- Evaluate your basic program
  - Do you have policies?
  - Is a risk assessment performed?
    - Has action been taken based on the risk assessment?
  - Is there an incident response plan?

Example – ePHI on mobile devices

Steps:
1. Identify all of the types and inventory of devices that contain ePHI
   - Who has it and do they need it?
2. What safeguards are on the devices?
   - Are they password protected?
   - Are the devices otherwise encrypted?
   - What if they are lost?
   - Remote wipe capabilities
   - Use of remote wipe capabilities ("I'm sure it's not lost...")
3. Have you tried to hack the device?
   - Intrusion and penetration testing can be worth the cost
4. Are there policies in place and has training occurred?
   - Do employees know what to do if they THINK the device is lost?

What happens if you have a security breach?

1. Reporting is expected — no “voluntary disclosure program.”
2. Coordinate with legal counsel
3. Pull the relevant policies
   - Is it too late to create policies?
4. Pull training records
   - Is it too late to do training?
5. Review security assessments and risk assessments
   - Security assessments performed on systems
   - Risk assessments to identify potential risk areas
   - Known, unaddressed risks are more “dangerous” than unknown risks
   - If something did not get addressed, why?
6. Do not forget state-specific privacy laws, e.g., California breach notification laws
Cybersecurity Threats & Mitigations

CyberSecurity Risk: 2017 Trends
- MOST at risk for Cyber threats: Financial (24%), Healthcare (15%), Retail (15%), and Public (12%)
- External threat agents (75%), Internal actors (25%) are responsible for the majority of the recent breaches.
- 66% of the breaches came from malicious email attachments
- Ransomware with cryptography is a lucrative attack technique for cyber criminals
- Internet of Things (IoT) growth serves as a popular attack vector for cyber criminals (ex: medical devices, refrigerators, Rx Dispensers, thermostats)

Compliance and CyberSecurity
- Cybersecurity refers to an organization’s ability to protect or defend the use of cyberspace from cyberattacks.
- Compliance and security are distinct disciplines often with shared objectives.
- You can be compliant without being secure and possible to be secure (relatively speaking – as no environment is ever completely secure) without achieving compliance.
- Threat analysis and comprehensive risk management should drive security priorities, and then be tested for compliance. This should be done rather than using compliance checklists to drive security.
- Effective Cyber Security Risk Management is upper management driven, selecting a risk framework, and executing on the strategic and tactical plans
Hacking – Threats & Risks

Computer hacking is the unauthorized intrusion or infiltration into a computer or a network. Hacker’s goal is to look for weaknesses to exploit, infiltrate the network, alter the software, circumvent the security measures of the computer or network, and/or obtain critical data.

A multi-layer security defense is essential to detect and prevent infiltration, but threats can still infiltrate porous layers.

Hacking – Strategies for Mitigation

Strategies for Mitigation:
- Use good system and network hygiene (disable default password, unused ports, update patches, strong passwords, limit permissions, disable remote access if not needed, no incident web browsing on servers)
- Perform penetration testing (third party or internal penetration tester)
- Continuous security incident monitoring and detection

Ransomware

Ransomware is a type of malware that prevents or limits use of a computer by locking the screen or the computer’s files until a ransom is paid. You may or may not get a decrypt key. Ransomware has evolved to using cryptography to hold data hostage without infiltrating your network, does not rely on command-and-control, and has the user to contact the bad guys for help.1

Ransomware – Strategies for Mitigation

**1 Bitcoin = $2,250 USD**

### Strategies for Mitigation:

- Plan ahead on who will pay and how to pay (Be realistic and make quick decisions)
- Check for description keys to recover your data (nomoreransom.org)
- Back up your data frequently and save to an alternative location (Backup servers in the data center or offsite location)
- Up-to-date patching and antivirus enabled for automatic update, where possible, on end-user devices and servers
- Limit network shares to folders and files and be vigilant on an individual’s permission rights (least privilege rule)

---

Phishing

- Phishing attack is an attack that cybercriminals use to fool you and collect valuable personal and financial information. Cybercriminals get you to click on a link from an email to redirect you to a suspicious website where you are prompted to enter your personal or financial information.
- Victims of phishing campaigns fall prey, repeatedly, even with additional training as a follow-up.
- Is 100% training compliance is equivalent to being secure?
- 95% of phishing attacks that led to a breach were followed by some sort of software installation. (Verizon DBIR 2017)
- A breach at DocuSign led to targeted email malware campaign in May 2017.

### Strategies for Mitigation:

- Use 2-Factor or Multi-factor authentication to access critical websites (ex. email, EML, financial data).
- Security Awareness & Training and applying the ‘Think Before You Click Rule’
- Phishing campaigns and awareness are effective when coupled with a negative consequence or a positive reinforcement.

---

**STAYING AHEAD OF CYBER RISKS**

- Identify and Prioritize your mission-critical assets and continuous maintenance
- Perform ongoing Vulnerability scanning and mitigation of prioritized vulnerabilities on mission-critical assets. The faster you identify vulnerabilities and execute a mitigation plan, you reduce the likelihood of an negative impact to the business.
- Execute Patch Management – deploy patches on systems with critical assets and reduce Patch cycles to days or as soon as possible.
- Continuous Audit logs & Security event monitoring
- Sharing information with other healthcare organizations
- Implement Incident Response plan and continuous exercise/testing
Thank you for attending.

Leeann Habte  
Partner  
Best Best & Krieger LLP  
leeann.habte@gmail.com  
(213) 787-2572

Darrell Contreras  
Chief Compliance Officer  
Millennium Health

Linh Sithihao  
Information Security Consultant  
Woodford Consulting, Inc.