Managing HIPAA Data Breaches

William J. Roberts, Esq.
June 15, 2016
Agenda

• What are the Risks of a Breach?
• Identifying Internal Threats
• Identifying External Threats
• Responding to a Data Breach
Data Breaches by the Numbers

$6.5 million – average cost of a data breach

11% - increase in cost between 2014 and 2015

$217 – average cost per lost or stolen record

112 million – number of individuals (U.S. only) affected by a health care data breach in 2015

432 million – number of hacked accounts (U.S. only) in 2014

Sources: (1) 2015 Cost of Data Breach Study: United States, Ponemon Institute Research; (2) Data Breaches In Healthcare Totaled Over 112 Million Records In 2015, Forbes, 12/31/2015
Data Breaches

• Breaches are increasing in sophistication, frequency and severity

• Health care is a primary target of breach activity and is subject to heightened government scrutiny and enforcement

• Threats can be categorized in two ways:
  ➤ External
  ➤ Internal
Identifying Internal Threats

• Insider threats are twofold:
  ➢ “Malicious Insider” – Wish to do harm to company
    ➢ Can be employee theft for personal or business gain
    ➢ Terminated employees taking data
    ➢ Accessing data outside scope of employment
    ➢ Employees purposely misusing data
Identifying Internal Threats

- Insider threats are twofold:
  - “Careless” or “Negligent” Insider
    - No ill will, but through carelessness, negligence or lack of training, creates openings for data loss
    - Employees are likely greatest threat to PHI
    - Includes lost files, laptops, mobile devices
Identifying External Threats

• External threats take two forms –
  ◆ An attack on your information systems or theft of physical files, or
  ◆ An attempt to trick an employee to divulge sensitive information
Cybersecurity – The Stats

Average *annual* number of cybersecurity incidents: 80 to 90 million

Increase in cybersecurity incidents from 2014 – 2015: 38%

Projected global cost of cyberattacks in 2019: 2.1 trillion US dollars

It’s Phishing Season!

- “Phishing” is an attempt to use email to trick a recipient into disclosing personal information, such as financial account information.
- We are seeing increased sophistication and volume of attempts.

“Masquerading” is a scam in which the perpetrator assumes the identity of a known, trusted colleague to trick the colleague into taking some action, often sending employee or financial data or wiring funds.

A Ransom for Your Data

• A ransomware attack is one in which a perpetrator assumes control of your data and will not release it until payment is made (or threatens to further disclose it unless payment is made)

• Payment is often requested in bitcoin
You’ve Been Hacked

• Hacking attempts are increasingly common in all industry sectors

• Healthcare, education, government, retail and finance are the most popular targets

• Small entities are just as likely (if not more likely) to be targets as large, well-known corporations

Source: Indianapolis Star, 12/15/14
Responding to a Data Breach

Discovery

Damage Control

Investigation

Mitigation

Notification(s)
Discovery

• Reporting Structure:
  - Incident notification policy
  - Employee/staff training
  - Culture of transparency, not fear
  - Consider mock breaches

• Need to have a breach response plan in place to guide response. Consider:
  - The Right Team: IT, compliance, HR, patient/public relations, legal counsel
  - Back-ups for each key, responsible individual (e.g. leave, vacation)
Investigation

- The covered entity must investigate the report of the breach without delay
  - Attorney-client privilege is vital to protect your interests
  - Have external resources lined-up ahead of time: PR, forensic IT, law enforcement contacts, external counsel
  - Only involve the necessary parties – confidentiality is important
Notification to Individuals

• **Rule:** Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information
  
  ✷ Notice must be written and sent by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically

  ✷ Notice must be provided without unreasonable delay and in no case later than 60 days following discovery

  ✷ Notice must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information
Notification to Individuals

• **Consider:**
  - Develop communication lines – toll free number, email, postal address
  - Who will respond to inquiries? Internal resources sufficient or call center needed?
  - FAQs
  - Language and disability concerns?
  - Minors?
  - Decedents?
  - Can you handle the communications in-house?
Substitute Notice

• **Rule**: Insufficient or out-of-date contact information for:
  
  - *10 or more individuals* - the covered entity must provide substitute notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside

    - must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach

  - *Fewer than 10 individuals* - the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means
Notification to the Media

- **Rule**: Covered entities that experience a breach affecting more than 500 residents of a state or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets
  - Often in the form of a press release
  - Without unreasonable delay and in no case later than 60 days following discovery
  - Must include the same information required for the individual notice

- **Consider**:
  - PR professional assistance
  - Media talking points
  - Media point person – who speaks for your organization (and who does not)
  - Controlling the message/coordinating with employees
  - Be cognizant of media leaks/stealth inquiries
Notification to HHS

- **Rule:** Covered entities must notify HHS by submitting a breach report form online
  - 500 or more individuals, covered entities must notify HHS without unreasonable delay and in no case later than 60 days following a breach
  - Fewer than 500 individuals, the covered entity may notify HHS of such breaches on an annual basis, due to HHS no later than 60 days after the end of the calendar year in which the breaches are discovered

- **Consider:**
  - Accuracy is vital
  - Summary statement may have significant consequences
Other Notification Obligations?

- Depending upon your sector, contractual arrangements or location, consider the following additional notifications that may be necessary:
  - State Attorney General(s)
  - State regulatory agencies (e.g. Departments of Health, Insurance or Consumer Protection)
  - Business partners (e.g. HIEs, affiliates)
  - Departments of Education (state and federal)
  - Political stakeholders (esp. if governmental entity)
  - Funders (look to grants, donors)
  - Employees (e.g. email, Intranet posting)
Thoughts on BA Breaches

• At times, a breach is caused by or occurs at your business associate. When planning for and responding to such a breach, consider:
  - BAA reporting, cooperation, mitigation and liability issues – is the BAA your friend or foe?
  - Who should notify?
  - Control of messaging
Mitigation

- **Rule**: A covered entity must take reasonable steps to mitigate harm to individuals caused by the breach
  - HIPAA is light on specifics but state laws are now mandating certain measures

- **Consider**:
  - What information can you provide to affected parties?
  - Credit monitoring – when? Required by law?
  - Credit counseling, identity theft recovery services
  - Identity theft insurance
Damage Control

• A data breach may inflict significant financial, operational and reputational costs on a company. Employee morale and confidence may also suffer. Develop a plan for:
  - Responding to questions and concerns from current and former employees, patients or customers
  - Handling inquiries from relevant business partners
  - Managing the company’s reputation in the business and consumer communities
Legal Risks

• Lawsuits Can and Will Come from Six Sources:
  ◆ Consumers
  ◆ Insurers
  ◆ Financial Institutions
  ◆ Shareholders
  ◆ Employees
  ◆ Government
Government Enforcement

- A HIPAA breach may result in enforcement actions from state attorney generals and the HHS Office for Civil Rights (OCR)
- In some instances, other enforcement agencies, including consumer protection, health, education or insurance departments, may have jurisdiction
  - Key – a HIPAA breach often violates other state and federal laws, meaning more opportunities for enforcement
Legal Risks and Government Enforcement

• Need to prepare for the following from “Day One”:
  - OCR investigation and enforcement action
  - Attorney General investigation and enforcement action
  - Lawsuits from patients, customers, business partners

• *Everything you do from preparing for the breach to your response to it is in preparation for these enforcement actions and lawsuits*
Penalties

- Recent changes to the law have significantly increased the penalties for violating HIPAA:
  - Four tiers of civil monetary penalties ranging from $100/per violation to $1.5 million/per violation
  - Criminal penalties: up to $250,000 in fines and up to 10 years in prison
- Both the covered entity and individual employees can be penalized for violating HIPAA
- Breaches may also result in costly consent orders or corrective action plans, lawsuits and additional penalties state enforcement actions
Learn from Others

• In 2014, New York-Presbyterian Hospital and Columbia University entered into settlement for $4.8M for failing to secure patient info

• Gov’t concluded companies:
  - Lacked technical safeguards
  - Failed to conduct accurate risk analyses
  - Failed to develop adequate risk management plans to address potential security threats
“Bad news, captain. The ship’s computer has been sharing all our personal data with the Romulans.”
Need Help With HIPAA Compliance?

- **The Guard**
  - Total Compliance Solution
  - Simple
  - Cost-effective
  - Compliance with Confidence

- **Support** - We work with you
  - Compliance Coaching
  - HIPAA Hotline
  - Education
  - Culture of Compliance

- **Contact Us**
  - 855 85 HIPAA (855-854-4722)
  - www.CompliancyGroup.com