Lessons Learned from Recent HIPAA and Big Data Breaches

Briar Andresen

Katie Ilten

Ann Ladd

Fredrikson & BYRON, P.A.

Recent health care breaches

- Breach reports to OCR as of February 2015
  - 1,144 breaches involving 500 or more individual
  - Over 157,000 breaches involving fewer than 500 individuals

HHS Wall of Shame

- Breakdown of breach by location
  - Paper records (22%)
  - Laptop (21%)
  - Desktop (12%)
  - Network server (12%)
  - Portable electronic device (11%)
  - Email (7%)
  - EMR (4%)
  - Other (11%)

HHS Wall of Shame

- Breakdown by type of breach
  - Theft (51%)
  - Unauthorized access/disclosure (19%)
  - Loss (9%)
  - Hacking/IT incident (7%)
  - Improper disposal (4%)
  - Other (9%)
  - Unknown (1%)

Anthem

- First reported to the media on February 4, 2015
- 80 million current and former members believed to be affected
- Multi-state breach
- Information breached
  - Name
  - Birthday
  - Street address
  - Email address
  - Medical ID and Social Security Number
  - Employment information (including income data)
- No credit card or medical information (claims, codes, test results) breached

Anthem

- “Sophisticated” attack on Anthem database
  - Speculation about foreign state sponsored hackers
  - Theory that malicious software was used to obtain an employee login
- Discovered when senior administrator noticed suspicious activity
- Source close to the breach says SSNs were not encrypted
- Certain hacked information tracked to outside internet storage site and locked down

Anthem

- Anthem originally planned to notify by email and/or letter
- Internet phishing attack followed
  - Targeted individual email accounts
  - Lured recipients to enroll in identity theft monitoring by providing financial info
- Anthem revised notice to send letters via USPS
- Offering free credit monitoring and ID protection services for up to 24 months
- One estimate said cost of breach is $200 per individual affected
- Class action lawsuits filed

St. Elizabeth's Medical Center

- July 2015 announcement of $218,400 settlement with OCR
- Incident discovered in November 2012
- Use of Internet-based document sharing application to store PHI of at least 498 individuals
  - No risk assessment
  - No business associate agreement
- Reported to OCR by a whistleblower
- Separate incident involving stolen flash drive with 595 patients' PHI

St. Elizabeth's Medical Center

- 12-month Corrective Action Plan
- Self-assessment and reporting on security vulnerabilities related to removal and transmission of ePHI, data encryption, and security incident reports
- St. Elizabeth's must conduct
  - Five unannounced site visits to assess compliance with policies and procedures
  - 15 random interviews with staff who have ePHI access rights
  - A minimum of three portable device audits to ensure data security measures have been addressed
- Interval reporting to OCR over the course of the 12-month plan

St. Elizabeth's Medical Center

- Employee use of cloud services
  - Employees at an average healthcare organization use a total of 928 cloud services, many without IT department's knowledge.
  - Average employee uses 26 cloud services.
  - Average healthcare organization uploads 6.8 TB of data to the cloud each month (Wikipedia archives = 5.64TB).
  - File-sharing services among top five uses.

--*Skyhigh Networks,* "93% of Cloud Services in Healthcare are Medium to High Risk," https://www.skyhighnetworks.com/cloud-security-blog/93-of-cloud-services-in-healthcare-are-medium-to-high-risk/.

Anchorage Community Mental Health Services

- $150,000 settlement announced in December 2014
- Breach involving unsecured ePHI of 2,743 patients
- Malware compromised security of IT resources
  - Periodic risk assessment lacking
  - Failure to update IT resources with available patches, resulted in vulnerabilities in firewall
  - Running outdated, unsupported software
  - Adopted sample Security Policies that were not followed

Illustrative non-health care breaches

- Target
- Home Depot

What have we learned?

- Data breaches are expensive
- Average cost of a data breach is $233 per record (Ponemon Institute 2013).
  - Legal
  - Computer forensic and investigation
  - Notification (mailing, postage, advertising)
  - PR consultant
  - Credit monitoring and identity theft services
  - Indemnification (for more than just mailing cost)

Data breach costs (cont.)

- Recovery costs (e.g., cost to restore access, loss of income)
- Investigation by government agency(ies)
- Resolution amounts
- Civil money penalties
- Lawsuits (possibly class action)
- Cyber terrorism related expenses

So much to worry about…what to care about the most?

- Security risk assessments
- Managing vendors
- Data breach response team and plan
- Employee training

Risk Assessment

- Part of any good security program
- Required under HIPAA
  - Also Meaningful Use
- Biggest failure, so says OCR
  - Failure to do it at all is a huge problem
  - Failing to have a complete assessment is a problem
  - Failing to follow through is a problem

Risk assessment: What's required?

- How do we actually do it/what should it look like?
  - 164.308(a)(1)(ii)(A): "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI."
    - Risk management
    - Sanction policy
    - Information system activity review
- Assign responsibility to a security official
- FLEXIBLE

Risk assessment

- Who should do it?
  - Internal team?
  - Outside vendor?
- What should it cover?
  - All of your PHI—electronic, but also your physical location, your devices, anywhere you have confidential information

Risk analysis must include:

- Potential risks/vulnerabilities to the confidentiality, availability and integrity of all e-PHI created, received, maintained, or transmitted
- Data collection
- Identify and document potential threats and vulnerabilities
- Assess current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of threat occurrence
- Determine the level of risk
- Finalize documentation
- Periodic review and updates

Risk analysis

- Keep going!
- When IT environment (or physical environment) changes, reassess
- If you find something, fix something
  - Put in place reasonable deadlines, then meet them

Managing Vendors

- Contracts- what's required under HIPAA, what else should you ask for?

HIPAA and Vendors

- Business associate agreements (BAAs)
- Have the BAA handy when there is a breach
- Must be written

Contracts with Vendors

Required BAA elements	Additional protections to consider, whether or not HIPAA applies
No use/disclosure of PHI other than as permitted or required by law	No use/disclosure of PHI (or any PII or other confidential information) other than as necessary to perform the vendor services
Use appropriate safeguards and comply with Security Rule	Provide contractually defined security measures, use industry standard security measures as they evolve, comply with law. May want to consider requiring outside certifications/audits

Contracts with Vendors (cont.)

Required BAA elements	Additional protections whether or not HIPAA applies
Report unauthorized uses and disclosures to covered entity	Report unauthorized access within [2] days, to allow customer to comply with state data breach notification laws AND to enforce contract rights
Ensure subcontractors agree to same restrictions as business associate	Equally applicable. And consider restricting use of subcontractors without consent.
Make PHI available for access	

Contracts with Vendors (cont.)

Required BAA elements	Additional protections whether or not HIPAA applies
Make PHI available for and incorporate amendments	Obligation to maintain current data as part of services
Make available information for an accounting	
Comply with Privacy Rule if carrying out covered function on behalf of covered entity	
Make internal practices, books, records related to use and disclosure available to Secretary	Consider customer right to audit/inspect facilities where data is hosted/managed

Contracts with Vendors (cont.)

Required BAA elements	Additional protections whether or not HIPAA applies
Return or destroy PHI at termination of contract	Right to access and receive copy of data (in xyz format) at termination of vendor services; maintain copy of data for no more than __days
Permit the covered entity to terminate if business associate has breached material term	Equally applicable, and consider defining certain types of security breaches as 'material'

Contracts with Vendors (cont.)

Required BAA elements	Additional protections whether or not HIPAA applies
	Indemnification for breaches of obligations regarding confidentiality and security
	Requirements around disaster recovery and back up
	Insurance that will cover costs related to breaches, other damages

Managing Vendors (cont.)

- Diligence- include security assessment for vendors?
  - Not *required*, but….
  - What are we looking for?
  - Examples-evidence that the vendor :
    - uses good physical security at any location where PHI is stored (access to data centers, fire suppression, backup)
    - Uses good network and systems security (firewalls, intrusion detection, vulnerability assessments, patching, audit logs)
    - Has good internal policies and procedures (training, background checking, a good security breach response policy)

Managing Vendors (cont.)

- How to conduct diligence-
  - Diligence questions/inspections
  - Manufacturer's Disclosure Statement for Medical Device Security (MDS2)
  - 3rd party standards/certifications
- What to do if a vendor screws up?

Managing Vendors (cont.)

- Diligence- include security assessment for vendors?
  - Not required, but….
  - How do we do it?
    - Diligence questions
    - Manufacturer's Disclosure Statement for Medical Device Security (MDS2)
    - 3rd party standards/certifications
- What to do if a vendor screws up?

Be prepared for a data breach

- What's the plan?
  - HIPAA – is it a breach??
    - Breach = the acquisition, access, use, or disclosure of protected health information in a manner not permitted under Privacy Rule of this part **which compromises the security or privacy of the protected health information**.
    - "not permitted" use/disclosure/access/acquisition is a **presumed breach**, but still must do risk assessment of factors

Is it really a HIPAA breach?

- Nature and extent of PHI involved (type of identifiers and likelihood of reidentification)
- Unauthorized person who used the PHI or to whom disclosure was made
- Whether the PHI was actually acquired or viewed
- Extent to which the risk to the PHI has been mitigated

Be prepared for a data breach

- HIPAA Notice
  - HIPAA requires notification of the individual and the Secretary for ALL breaches
    - Annual reporting to the Secretary unless it is a breach affecting 500+ individuals
    - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
  - Media notice if breach affecting 500+

Be prepared for a data breach

- What else?
  - Identify response team and outline roles and responsibilities
  - List strategic partners (legal team, PR firms, computer forensics experts, law enforcement, credit monitoring, call centers, etc.)
  - Explain when/how the board and key stakeholders within the company will be informed of the breach

Employee training

- It is required under HIPAA
- In healthcare, about 1/5 of all data breach incidents are based simple human error
- Train people how to securely send, store, and dispose of PHI

What to expect if you have a problem

- OCR investigation
  - Based on complaint, breach report, audit
  - Usually starts with a letter, asks for info/explanation
  - Keep good notes, keep timeline
  - Most resolved without major issues
  - If there IS a major issue, OCR will send letter with resolution amount, resolution agreement
- Other federal and state level investigations, actions, and private actions

HIPAA Audit Program

- Required by the HITECH Act
- Phase 1 over (audited 115 covered entities)
- Phase 1 lessons
  - Lack of thorough risk analyses
  - Failure to comply with breach notification rule

HIPAA Audit Program

- Phase 2
  - Randomly selected pool of covered entities received preliminary surveys in May 2015
  - 150 covered entities and 50 business associates to be audited
- Differences in Phase 2
  - Will expand focus to covered entities and business associates
  - Data requests will seek contact information for business associates
- Purpose is to identify best practices, develop technical assistance, and uncover risks and vulnerabilities.
- Audit could lead to formal compliance review by OCR.

Low hanging fruit

- IT
  - Known but unpatched vulnerabilities
  - Not using encryption
- Employee behavior
  - Not shredding
  - Passwords on post-its
  - Laptops visible in car
  - Phishing and other scams

Low hanging fruit (cont.)

- Insurance coverage
  - Most professional malpractice carriers have an automatic coverage for cyber liability, but limits are inadequate
  - General Liability may not cover
  - Consider cyber liability coverage.
    - First-party coverage addresses expenses due to breach, including forensics, notification/response, crisis management, and data loss.
    - Third-party coverage addresses liability to third-parties from litigation against insured following a breach.

Questions?

Briar Andresen
(612) 492-7057
bandresen@fredlaw.com

Katie Ilten
(612) 492-7428
kilten@fredlaw.com

Ann Ladd
(612) 492-7124
aladd@fredlaw.com