Cutting Through the Noise: Determining Whether Your Vendor's Security Incident Is a Breach

Session 701
23rd Annual Compliance Institute
Boston, MA
April 9, 2019

Thora Johnson, Esq.
Chair, Healthcare Practice
Venable LLP
TAJohnson@Venable.Com

David Holtzman, JD, CIPP
Executive Advisor
CynergisTek
david.holtzman@cynergistek.com

Shari Lewison, MBA, CISA
CISO
Univ. Iowa Hospitals & Clinics
Shari-lewison@uiowa.edu

Attacks On Healthcare Increasing

- First quarter of 2018, the healthcare sector is the top-targeted industry*
- Increasing attacks since 2015*
- Reasons why
  - Highly valuable data (10x more than credit card number)
  - Lack of IT investment and thin margins
  - Highly connected systems with many participants
  - Push for interdependence and interconnectedness
  - Outdated software and devices**
  - Vulnerability management issues**

*Rapid7 Quarterly Threat Report

**Energy and Commerce Committee Report

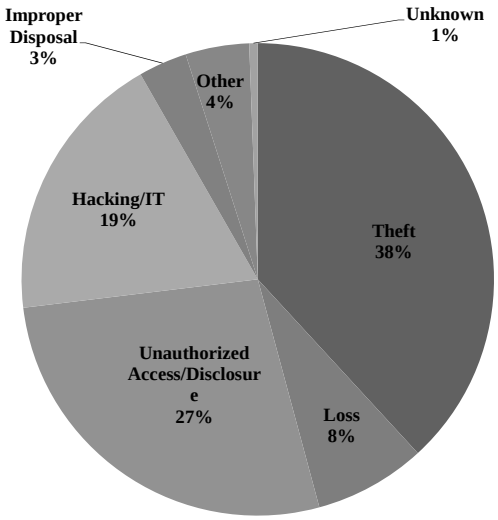
Costs Of Data Breach In Healthcare

- Cross-industry average cost of data breach is $148 per record lost
- In healthcare, jumps to $408 per record
- Highest of any industry, followed by financial services
- What are these costs?
  - Detection and escalation
  - Notification costs
  - Post data breach response
  - Lost business

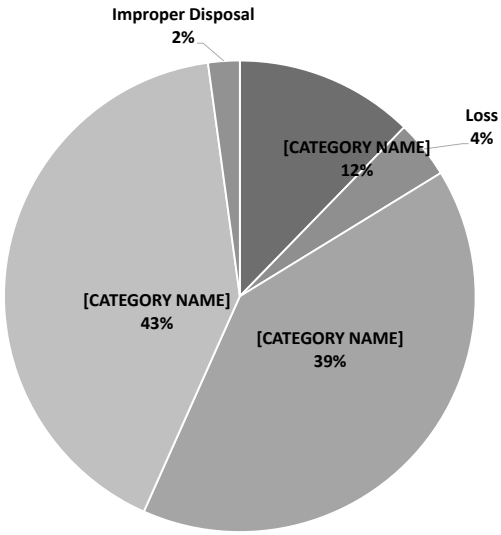
2018 Cost of Data Breach Study – Ponemon Institute

500+ Breaches by Type

September 23, 2009 through December 31, 2017



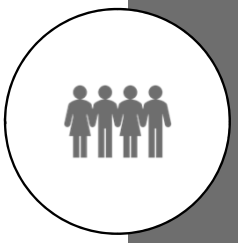
January 1, 2018 through December 31, 2018



4

Business Associates & Breaches

- 393 breaches affecting > 500 individuals reported to OCR in 2018
- 25% of these large breaches reported to have involved a business associate
- 2.65 million patients affected by breach of business associate that was providing billing and payment services
- $16 million penalty paid to OCR settling HIPAA violations by insurer and TPA arising from breach affecting 79 million



HIPAA's Approach To BAs: An Evolution

- Privacy Rule: Protect against unauthorized uses & disclosures to protect the privacy of PHI
- Security Rule: Risk Analysis and Risk Management Plan
- Both: Obtain satisfactory assurances that business associate "will appropriately safeguard" PHI in the form of a business associate agreement
- If covered entity knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligations, the covered entity must take steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the contract, if feasible
- And, as of HITECH, business associates have direct liability for CMPs for certain violations of the Privacy Rule and any violation of the Security Rule

BA's May Pose Information Security Risk To CEs

- OCR Guidance on Cloud Computing implies that CE has a role in managing BA
  - "A covered entity (or business associate) that engages a CSP should understand the cloud computing environment and solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate BAAs."
  - And, while guidance specifically states that CSPs are not required under HIPAA to provide documentation, or allow auditing, of their security practices, it notes:
    - Customers may require a CSP through the business associate agreement, service level agreement or other documentation to provide documentation of safeguards or audits, based on the customer's own risk analysis and risk management or other compliance activities

https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

OCR Enforcement Involving BA

- Hospital received centralized IT services from its corporate parent
- Hospital and parent had entered into an agreement designating them an ACE
- Two backup tapes containing PHI of over 14,000 individuals were discovered missing
- No BAA in place until after OCR initiated its compliance review
- Resolution agreement and CAP, including payment of penalty of $400,000

https://www.hhs.gov/sites/default/files/9-14-16-wih-racap-1.pdf

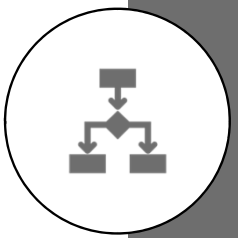
New Enforcement by State AGs

- NJ AG fined medical group $418,000 for 2016 breach involving BA
- Medical transcription vendor misconfigured the medical group's FTP server that exposed PHI of 1,600 patients on Internet
- AG's investigation found that:
  - The vendor failed to notify the medical group of the incident resulting in failure to timely notify impacted individuals and the state of the breach
  - Medical group failed to exercise appropriate oversight of the vendor's security practices in safeguarding PHI

https://nj.gov/oag/newsreleases18/Virtua-Medical-Group-Consent-Judgment.pdf

Are BA's Prepared For Security Incidents?

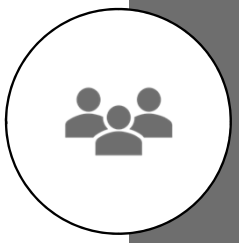
"Despite the requirements of HIPAA, not only do a large percentage of covered entities believe they will not be notified of security breaches or cyberattacks by their business associates, they also think it is difficult to manage security incidents involving business associates, and impossible to determine if data safeguards and security policies and procedures at their business associates are adequate to respond effectively to a data breach."



OCR Cyber-Awareness Monthly Update – May 3, 2016

So…What Can You Do To Be Proactive?

- Identify who is (and who is not) a business associate
- For those who are business associates, know:
  - Their names
  - Their mailing address and where they operate
  - Two points of contact for each
  - URL of their websites
  - Their services
  - The PHI involved and how it is used/disclosed



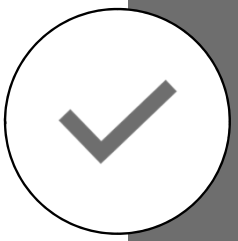
Managing Vendors To Reduce Risk From BAs

Conduct initial and ongoing due diligence

- Audits and questionnaires
  - Risk introduced by the vendor
  - Type and volume of PHI
  - Criticality of vendor's functions
- Know
  - How they address risks of subcontractors
  - Whether they use offshore subcontractors
- Require
  - Written privacy and security policies
  - Risk analysis and risk mitigation plan
  - An incident response plan
  - Business continuity and disaster recovery plan
  - Training and sanction policy

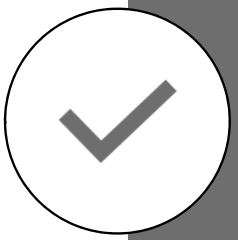
BA Agreements Rights & Responsibilities

- Enter into business associate agreements that:
  - Incorporate the right to perform ongoing due diligence
  - Require notification of all impermissible uses and disclosure of PHI, including security incidents and breaches of unsecured PHI
    - Consider timing – if breach, without undue delay but not more than 60 days from discovery
    - But, does that timing seem appropriate?
  - Require cyber insurance for companies that may not be able to indemnify otherwise
  - Permit termination



BA Agreements Rights & Responsibilities

- Enter into business associate agreements that address:
  - Responsibility for determining breach (see next slide)
  - Information to be reported – and how and when and to whom
  - Duty to report to affected individuals and OCR (and state officials)
  - Right to review and approve any notifications
  - Mitigation, cooperation, and insight into the business associate's response and systems (information sharing)
  - Costs and indemnification



Breach?

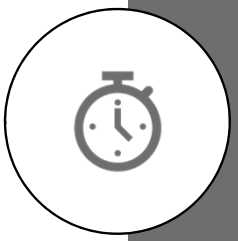
- HIPAA: Acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of PHI
  - There are few exceptions
  - Otherwise, any impermissible use or disclosure of unsecured PHI is presumed to be a breach unless you can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment
    - Nature & extent of PHI involved
    - PHI actually acquired or viewed
    - Unauthorized person who used PHI or to whom it was disclosed
    - Extent of mitigation

Breach?

- But HIPAA is not the only potentially applicable breach standard to be considered
- There is a patchwork of state breach notification laws that may apply
  - Reporting deadlines may differ
  - Content of notice may differ
  - Notice to state regulatory bodies may be necessary
- State data breach assessment & notification requirements are in addition to HIPAA

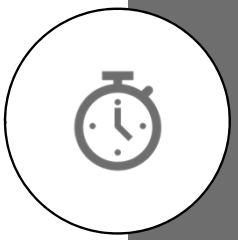
What To Do When the Inevitable Occurs

- Activate your incident response plan – Immediately!
- Determine how and when to probe
- Who to involve at early stage of investigation (think small)
  - Legal counsel (in-house and outside counsel)
  - CISO and IT
  - Privacy officer and chief compliance officer
- Contain and mitigate
- Establish cadence of status reports
- Review the vendor agreement and BAA
- Determine form of vendor reports



What To Do When the Inevitable Occurs

- Require preservation of evidence for forensic analysis, if necessary
- Identify needed documentation, if any, to conduct a root cause analysis
  - Description of what happened, including the date of the incident and the date of discovery and investigative steps
  - Inventory of data
  - Forensic reports
- Determine whether law enforcement should be notified
- Report cyber threats to federal and information-sharing and analysis organizations



Reporting And Recovery

- Determine HIPAA and state reporting obligations, if any
  - If reporting, determine if PR firm is necessary and potentially establish call center
  - Document beach risk assessment, even if no reporting
- Log improper disclosures, if necessary for accounting purposes
- Re-evaluate relationship with vendor
- Take stock of lessons learned from incident

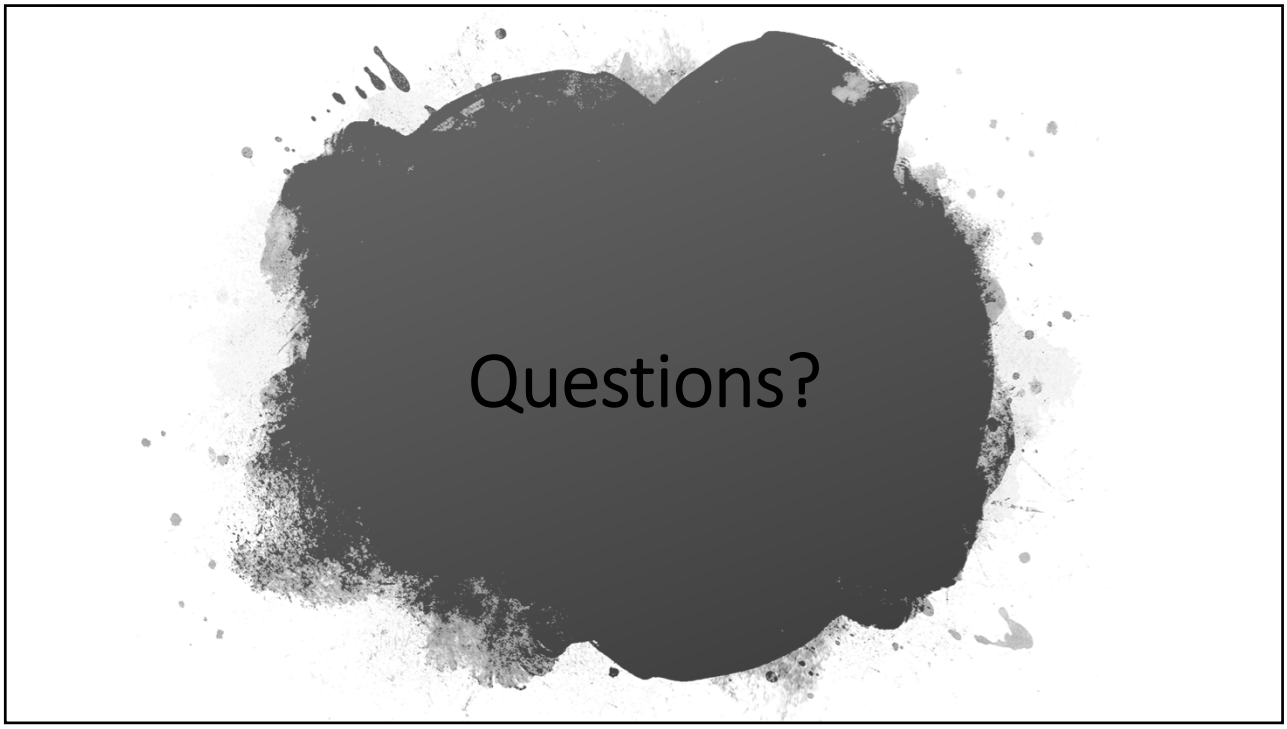
What To Expect Tomorrow

More focus on vendor management

More OCR enforcement

More AG enforcement

More litigation


Questions?