302 The Blame Game: Accountability in Healthcare Compliance

Rick Kam
President and Co-Founder
ID Experts

Learning Objectives

- Blame Game: Covered Entity versus Business Associates
- What a business associate agreement should include
- What to do to be prepared before a data breach
- Responding to a data breach

What Not Covered?

- Not providing legal advice
- Cyber security best practices
- Compliance with HIPAA Security/Privacy rules
- Other

What is a Data Breach?

Data Breach is a "Legal" Construct

All breaches start as incidents, but not all incidents end up as breaches

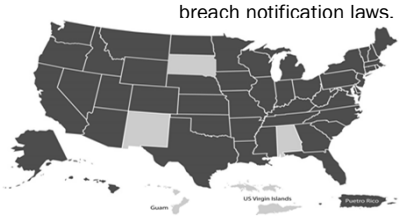
"Incident" = attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI/PII

"Breach" = acquisition, access, use, or disclosure of PHI/PII [that poses a significant risk of financial, reputational, or other harm]*

*The definition of "data breach" varies across specific legislation and rules. In US states, many include a "harm threshold"

Complex Web of Breach Laws

Organizations that hold regulated data must comply with data breach notification laws.



Data Breach Notification Laws:

- 47 state laws
- 3 U.S. territories
- HIPAA Final Breach Notification Rule
- Gramm–Leach–Bliley Act (GLBA)

Healthcare is a Prominent Target

Industries Affected by Data Breaches:

Healthcare	26.9%
Education	16.8%
Government	15.9%
Retail	12.5%
Financial	9.2%
Service	3.5%
Banking	2.8%
Technology	2.6%
Insurance	1.6%
Media	1.4%
Others	6.8%

Source: TrendMicro, *Follow the Data: Analyzing Breaches by Industry*, 2015

id experts

Why Target Health Data?

Why hackers are targeting health data:

- **Value.** Health data on the black market is more valuable than other kinds of personal and financial data
- **Vulnerability.** Organizations with health data, including third parties, have less mature security postures compared with financial firms
- **Scale.** With an APT, there is the ability to acquire massive amounts of data

id experts

The Costs Are Still Rising…

Average organizational cost of a data breach: $7.01 Million

- Up 130% in 2 years

The cost per record can vary based on root cause of breach:

- Malicious or criminal attack = $236
- System glitch = $213
- Human error = $197

*IBM/Ponemon Institute, *2016 Cost of Data Breach Study*

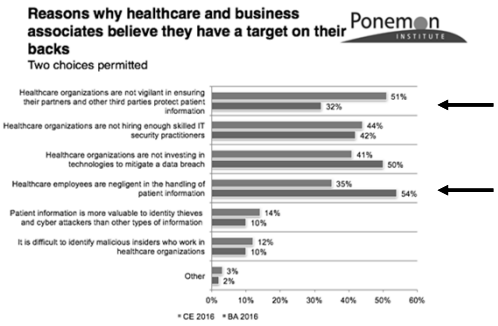
Blame Game

Protecting PHI not improving…

Third Parties Increase Risks

- 41% of healthcare data breaches were caused by third-party snafus
- Third parties are often negligent in the handling of sensitive data, lacking resources, technology, and processes
- Legal responsibility lies with the covered entity

id experts



What a BAA Includes?

A Written contract that defines responsibilities between CE and BA that helps mitigate BA risk

1. Permitted and required uses of PHI
2. Not further disclose PHI
3. Implement appropriate safeguards for PHI
4. Report breach of PHI
5. Provisions to increase collaboration on pre-breach readiness

https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Mitigating Financial Risk: Cyber Insurance

- What does your policy cover?
  - First party losses and costs?
  - Third party costs?
  - Remediation costs?
  - Fines and penalties?
  - Risk management services?
- What is the retroactive date?
- What does your policy allow you to choose?
  - Selection of outside counsel?
  - Selection of breach responders?
- Do the limits of liability match your exposure?

Strategies for Mitigating Operational Risk

- Conduct inventory of all hardware and software
- Use current version of operating systems
- Automate security patching
- Enable intrusion detection & prevention systems
- Segment network
- Control access based on need to know
- Require complex passwords & use multi-factor authentication
- Eliminate unnecessary data and processes
- Protect data
- Monitor endpoints
- Conduct due diligence on all third party service providers
- Conduct join risk assessments
- Conduct vulnerability testing and audit
- Develop incident response plan & test the plan
- Conduct employee training on network security awareness
- Common risk assessment methodology

Future Predictions

- IoT will provide basis for attacks on attached devices of all kinds
- Ransomware will continue to be successful in targeting healthcare
- Medical device and wearable hacks will surface soon
- Growth in cybercrime-as-a-service make attacks viable for less sophisticated actors

Questions?

Rick Kam
President and Co-Founder
ID Experts
971-242-4706
Rick.kam@idexpertscorp.com