61st Annual Employee Benefits Conference

How To Survive A Cybersecurity Breach

Wyatt Holliday, CEBS
Attorney
Shumaker, Loop & Kendrick, LLP
Toledo, Oh

David Coney, CIC
Vice President
Union Insurance Group
Chicago, IL

International Foundation of Employee Benefit Plans
Education | Research | Leadership

Topic Overview

- Business Associate Agreement Provisions
- Communicating With Affected Parties
- Fiduciary Insurance Policy Issues
- Who Is Liable?
- Vendor Contract Provisions
- Curing The Breach

Business Associate Agreement Provisions

- What does a BAA do?
  - Lays out the rights and responsibilities of the Covered Entity (the health plan) and the Business Associate.
  - Contains security, administrative and notification provisions governing the CE and BA's actions and communications

Business Associate Agreement Provisions

- Who is a business associate?
  - Performs or assists in performing activity that
    - Uses or discloses health information
    - Provides professional services involving disclosure of such information
    - (Legal, accounting, management, consulting, etc.)
    - 45 CFR 160.103
  - Business associate has same civil/criminal exposure as covered entity

Business Associate Agreement Provisions

- HITECH (2013) required certain changes in BAAs impacting cyber security:
  - Add "creates, receives, maintains or transmits" to the section describing BA receiving data from or producing data for CE
  - BAA must provide that any sub-BAA is at least as stringent as the one between CE and BA
  - Business associate must report breach in accordance with 45 CFR 164 Subpart D "without unreasonable delay"; but including definition of that in BAA suggested.
    - Statutory 60-day limit impacts plan's ability to react appropriately.
  - If BA is performing CE's obligation under privacy rule, BAA must require that BA abide by privacy rule.

Communicating With Affected Parties

- State and Federal Breach Notification Laws
  - 47 States, DC, Puerto Rico, USVI and Guam have enacted legislation requiring the notification of individuals affected by security breaches of personally identifiable information (PII)
  - www.ncsl.org – search on "Security Breach Notification Laws"

- US Dept. of Health & Human Services
  - HIPAA Breach Notification Rule – 45 CFR 164.400-414
    - Requires HIPAA covered entities and business associates (i.e. TPA) provide notification following a breach of unsecured protected health information (PHI)

- Federal Trade Commission
  - Applies to vendors of personal health records and their third party administrators
  - Doesn't apply to business or organizations covered by HIPAA
  - Pursuant to section 13407 of the HITECH Act
  - Health Breach Notification Rule
    - Notify everyone whose information was breached
    - In many cases, notify the media
    - Notify the FTC

Communicating With Affected Parties

- Notifications required when breach related to Protected Health Information (PHI)
  - Individual Notice
  - Media Notice
  - Notice to Secretary, Health & Human Services
  - Notification by a Business Associate

Communicating With Affected Parties

- Individual Notice
  - Written Form – 1st Class Mail or e-mail if affected person agreed to receive such notices electronically
  - Have inaccurate contact information for 10 or more people?
    - Posted on their website home page for at least 90 days or
    - Provide notice in major publication or broadcast media for at least 90 days in region where affected individuals likely reside
  - Must include toll-free number, be active for 90 days, where individuals can learn if their information was affected
  - Provided without unreasonable delay – no more than 60 days following discovery of breach

Communicating With Affected Parties

- Individual Notice – must include:
  - Brief description of the breach
  - Types of information involved
  - Steps individuals should take to protect themselves from potential harm
  - Description of what the fund is doing to
    - Investigate the breach
    - Mitigate the harm
    - Prevent further breaches
    - Include Fund contact information
  - Fund is ultimately responsible for ensuring affected individuals are notified

Communicating With Affected Parties

- Media Notice
  - Required if more than 500 residences of a State or jurisdiction are affected
  - Sent to prominent media outlets serving the State or jurisdiction, typically in the form of a press release
  - Provided without unreasonable delay – no more than 60 days following discovery of breach
  - Same content as Individual Notice

Communicating With Affected Parties

- Notice to Secretary, HHS
  - Required if breach is of unsecured protected health information (PHI)
  - Notify via HHS website: submit electronic breach report
  - 500 or more affected individuals, must notify within 60 days
  - Less than 500, may notify on an annual basis, but no later than 60 days after the calendar year in which the breach occurred

Communicating With Affected Parties

- Notification by a Business Associate
  - Notify Fund after discovery of breach without unreasonable delay, no more than 60 days
  - Provide Fund with identification of each individual affected by the breach – to the extent possible
  - Any other information required by the Fund

Fiduciary Insurance Policy Issues

- Fiduciary Liability policy not written for cyber liability coverage
- Cyber Liability endorsements provide limited coverage
  - Rarely cover breach notification, crisis management and response expenses
  - Often sub-limited to fraction of the policy limit
- Cyber Liability Breach Coverage
  - 1st Party Expense Coverage – none or limited
  - 3rd Party Expense Coverage – sub-limited

Fiduciary Insurance Policy Issues

- Cyber Liability – First Party Coverage
  - 1st Party Breach Response
    - Pre-claim counsel
    - Crisis management
    - Notification expense including credit monitoring
    - Computer forensics
    - Call center services
  - Fines and Penalties Assessed By
    - HIPAA/HITECH
    - Payment Card Industry (PCI)
    - State regulators
  - Other First-Party Insurance
    - Loss of data from computer disruptions
    - Restoration costs
    - Business interruption
    - Cyber extortion, computer fraud, funds transfer fraud

Fiduciary Insurance Policy Issues

- Cyber Liability – Third Party Coverage
  - 3rd Party Liability
    - Information Security and Privacy Liability
      - Legal liability, defense costs and expense reimbursement
    - Network Security Liability
      - Failure to prevent security breach
    - Website Media
      - Liability for online media activities
        - » Defamation, copyright and trademark infringements
    - Judgements / Settlements
    - Defense Costs – Litigation
    - Defense Costs - Regulatory

Who Is Liable?

- Liability attaches to:
  - Covered Entity

  And since the HITECH Act,
  - Business Associate
  - Business Associate's Business Associate

- Everyone is equally liable!
  - HITECH likened CE/BA relationship to that of an agent, so any lawsuit against BA would likely hold CE responsible

Who Is Liable?

- Liability can include:
  - Sanctions under HIPAA's privacy and security rules
  - Sanctions under various state laws
    - 47 States plus DC, Puerto Rico, USVI and Guam
  - Civil lawsuits
    - HIPAA privacy and security rules can be cited as "best practices," so a violation can form the basis for a tort suit

Who Is Liable?

- Monetary Penalties:
  - $100 to $50,000 per violation, depending on the level of culpability
  - $1.5 million cap per calendar year for multiple violations of identical provisions
- Criminal penalties of up to 10 years' imprisonment
- Willful neglect is frowned upon.
  - Even a possibility of a violation due to willful neglect can impose civil monetary penalties
- 45 CFR 160.400 *et seq*

Who Is Liable?

- Cyber Liability versus Fiduciary Liability
  - Nothing is 100% secure
  - The FBI told congress that the Sony hack would have defeated 90% of the security out there.

- A cyber breach only becomes a fiduciary breach if a <u>prudent individual familiar with cyber security</u> would not have done what the Plan Administrator did.
  - National Initiative for Cybersecurity Education (NICE) report says cyber security is "much more than technological solutions to technical problems; it is also highly dependent on educated users who are aware of and routinely employ sound practices when dealing with cyberspace."

Who Is Liable?

- Sound internal practices
  - Data security
  - Physical security
  - Personnel management
- Due diligence on external practices
  - Boards of Trustees are (probably) not e-security experts.
  - They can ask the right questions.

Who Is Liable?

- "Surviving" means a lot of things
- How does your client look in the letters/press releases/news stories?
- "We did everything would could to protect your privacy."

Vendor Contract Provisions

- BAs have same liability as CE; useful basis for looking at all vendor contracts.
- Vendors should maintain their own cyber liability insurance, because ….
- DOL hot-button: Limitations of Liability
  - DOL Advisory Opinion 2002-8A
  - LoL/indemnification not *per se* imprudent or unreasonable, <u>BUT</u>
  - Provisions re: fraud/willful misconduct void as against public policy

  - <u>AND</u>

Vendor Contract Provisions

- Provisions limiting liability or indemnifying for negligence or unintentional malpractice are ONLY reasonable if:
  - Such provisions are reasonable in context AND
  - The fiduciaries have assessed comparable services at comparable costs from alternate vendors who do not require such terms or who provide greater protection to the plan.
- The plan MUST put any such contract out to bid!

Curing The Breach

- Develop a robust data security and incident response plan before you have a cybersecurity breach
  - National Institute of Standards and Technology (NIST) provides a framework on managing and reducing cybersecurity risk
    - Identify – information assets and risks, set priorities, perform vulnerability tests
    - Protect – implement security procedures, hardware/software, staff to manage and monitor
    - Detect – monitor network traffic, servers, laptops, smartphones 24 hrs a day
    - Respond – get cybersecurity experts involved immediately. The sooner you get the attackers out, the overall less cost to cure
    - Recover – Incident Response Plan, Business Continuity Plan

- Purchase a robust Cyber Liability insurance policy
  - Instant access to IT forensic experts and data breach legal experts
  - Infrastructure to deal with member notification, information phone bank, credit monitoring
  - Public relations support
  - A dedicated limit of insurance tailored specifically to cover cyber breach 1st and 3rd party expenses
  - Often provide web links to resources for the development of Data Security & Incident Response Plans

- Timely response is critical!
  - Average time to respond to a cyber attach is 45 days
  - Average cost of $1.6 million
  - The longer it takes to respond, more data is lost and greater the cost to recover

Key Takeaways

- A fiduciary liability policy, even with endorsements, leaves significant gaps; a cyber liability policy comprehensively covers your response to a breach.
- Learn the right questions to ask in due diligence – due diligence may mitigate liability!
- Make sure your clients are not unintentionally indemnifying vendors and service providers.
- Develop, implement and maintain a robust data security and incident response plan NOW!