Beyond HI PAA: Data Security and the Benefit Plan

Sarah Bhagwandin
Counsel
Bryan Cave LLP
Denver, Colorado
The Benefit Plan and Risks to Data

• Standard Data Security Programs often miss employee benefit plans.

• What data is at risk?
  • Employee names
  • Addresses
  • Social security numbers
  • Birthdates
  • Hire dates
  • Retirement dates
  • Compensation information
  • Asset balances

• What are the unique challenges to safeguarding benefit plan data?
Data Security and the Benefit Plan – Beyond HIPAA:

Today’s Agenda

I. Overview of Current Data Security Climate
   A. Breach Statistics
   B. Regulatory Climate
   C. Lessons from HIPAA – Roadmap to a Gap Analysis

II. Data Security and Fiduciary Liability
   A. Is cyber security an ERISA plan fiduciary responsibility?
   B. Applying ERISA plan fiduciary principles to cybersecurity

III. Cyber Security: Fundamentals of an Effective Strategic Plan
Breach Statistics for PHI:
September 2009 through May 31, 2017

- Approximately 1,945 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 49% of large breaches
  - Hacking/IT now account for 16% of incidents
  - Laptops and other portable storage devices account for 26% of large breaches
  - Paper records are 22% of large breaches
  - Individuals affected are approximately 173,594,541

- Approximately 288,256 reports of breaches of PHI affecting fewer than 500 individuals

Retrieved from United States Department of Health & Human Services, Office for Civil Rights; HIPAA Breach Highlights.
## Big Health Industry Breaches
(Over 1 Million Records)

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Type of Event</th>
<th>Number of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anthem</td>
<td>Hacking/IT Incident</td>
<td>78,800,000</td>
</tr>
<tr>
<td>Premera Blue Cross</td>
<td>Hacking/IT Incident</td>
<td>11,000,000</td>
</tr>
<tr>
<td>Science Applications International Corporation</td>
<td>Loss involving</td>
<td>4,900,000 (BA)</td>
</tr>
<tr>
<td>Community Health Systems Professional Services Corporation</td>
<td>Theft involving 4,500,000 (BA)</td>
<td></td>
</tr>
<tr>
<td>Advocate Health and Hospitals Corporation</td>
<td>Theft involving 4,029,530</td>
<td></td>
</tr>
<tr>
<td>Xerox State Healthcare, LLC</td>
<td>Unauthorized Access/Disclosure</td>
<td>2,000,000 (BA)</td>
</tr>
<tr>
<td>GRM Information Management Services</td>
<td>Theft involving 1,700,000 (BA)</td>
<td></td>
</tr>
<tr>
<td>AvMed, Inc.</td>
<td>Theft of Laptop involving 1,220,000</td>
<td></td>
</tr>
<tr>
<td>Montana Department of Public Health and Human Services</td>
<td>Hacking/IT Incident</td>
<td>1,062,509</td>
</tr>
<tr>
<td>BlueCross BlueShield of Tennessee, Inc.</td>
<td>Theft of services involving 1,023,209 (BA)</td>
<td></td>
</tr>
</tbody>
</table>

“BA” = Business Associate
Data Security and the Benefit Plan: Regulatory Climate

  - 2016 – “Cybersecurity Considerations for Benefit Plans”


- Federal Law
  - There is no comprehensive federal law governing cybersecurity for benefit plan providers
  - HIPAA
ERISA Advisory Council Reports

- Cybersecurity Considerations for Benefit Plans
  - November 2016
  - Focused on outlining cyber risk management strategies for plan sponsors

- Privacy and Security Issues Affecting Employee Benefit Plans
  - November 2011
  - Identifies risks to information maintained by plans
Issues Identified in Testimony to 2016 Council

- Can the DOL clarify whether ERISA pre-emption applies to state laws governing cybersecurity?

- **DOL should provide either:**
  1. Regulations that will create a single, national breach reporting standard for all employee benefit plans; or
  2. Guidance that will provide plan administrators better clarity regarding whether cyber risk security is a fiduciary priority or not? If yes:
     - Just how much of a priority is it?
     - Are there certain minimum steps that should be taken?
     - Consider a framework mandate or guidance
     - Finally, as ERISA mandates fiduciaries try to minimize administrative expenses,
        1. Should cyber liability insurance be considered?
        2. Will the cost of cyber liability insurance be a reasonable plan expense?
        3. Given the growth, prevalence, and potential disastrous consequences of a significant cyber breach event, could the lack of cyber liability insurance ever be considered a breach of fiduciary duty?
Data Security and the Benefit Plan: The Regulatory Climate

Federal Law – HIPAA

- Introduced a framework for building a privacy and security plan
- Created uniform federal standards for treatment of health information
- Created federally protected rights
- Imposed federally-based obligation to protect personal information
Data Security Climate: HIPAA – A Template?

- **Privacy Rule**: Protects all forms of PHI (oral, electronic, paper)
- **Security Rule**: Protects integrity, confidentiality, and availability of health information
- **Framework**:
  1. Privacy Officer/Security Officer (ownership)
  2. Privacy Notice and complaint procedure (disclosure)
  3. Risk Assessment and Risk Management Plan (examine specific setting)
  4. Administrative, Physical and Technical Safeguards (address risks)
  5. Policies and Procedures (integrating thoughtful best practices)
  6. Personnel Training (integrating practices & ethics in workflow)
  7. Business Associate Contracts (exposure to 3rd parties/shift liability)
Data Security Climate: Lessons from Gaps in HIPAA Compliance

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threats
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Retrieved from United States Department of Health & Human Services, Office for Civil Rights; HIPAA Breach Highlights.
Data Security Climate: Anecdotal HIPAA/HITECH – “Red Flag” Issues

- Inadequate encryption policies and procedures
- Poor access control and activity review
- Poor mobile device and laptop policies and controls
- Lack of IT governance – standards, inventory control, basic security procedures (patching, administrative lockdown, etc.)
- Inadequate disaster recovery procedures
- Insufficient IT policies and procedures
- Lack of advanced monitoring techniques – intrusion detection system/intrusion prevention system (IDS/IPS), log correlation, data loss prevention (DLP)
- Lack of a security officer
Data Security Climate: Common Corrective Action Recommendations

- Update risk analysis and risk management plans
- Update policies and procedures
- Training of workforce
- Implement specific technical or other safeguards
- Mitigation
II. Data Security and Fiduciary Liability

A. Is cybersecurity an ERISA plan fiduciary responsibility?

B. Fiduciary Principles – Applied to Cybersecurity
Data Security and Fiduciary Liability

- The 2016 ERISA Council Report noted that because employee benefit plans are generally regulated by ERISA, the breaches of participant data implicates the rights and duties of plan fiduciaries and service providers arising under ERISA, as well as possibly implicating state data protection laws.

- The Report notes “ambiguities and potential issues remain with regard to whether cybersecurity is a fiduciary responsibility as well as whether state cyber laws are preempted by ERISA.”

- The 2016 Council determined that providing guidance on those topics was beyond the scope of its study.
Who is a Fiduciary?

- Under ERISA, a fiduciary is a person who:
  - Is the “named fiduciary” (a formal designation by the plan — plan administrator and trustee, typically)
  - Exercises discretion with respect to management or administration of the plan
  - Exercise discretion with respect to the management or disposition of plan assets, or
  - Provides investment advice for a fee
- Functional test focuses on actual control and authority over plan
What is the Significance of Being a Fiduciary?

• ERISA fiduciaries are subject to heightened standards of conduct because they are acting on behalf of the plan participants and beneficiaries.

• If a fiduciary fails to comply with the applicable standard of conduct, he or she may be held personally liable for, among other things, any plan losses resulting from the breach.

• Fiduciary liability is joint and several.
General Fiduciary Requirements ERISA § 404(a)(1)

- A plan fiduciary has the following affirmative duties:
  
  1. Duty to act prudently (prudent “expert” rule)
  2. Duty to diversify the assets of the plan to minimize the risk of large losses
  3. Duty to comply with the provisions of the plan documents to the extent consistent with ERISA
  4. Duty of loyalty – to act solely in the interest of participants and with the exclusive purpose of providing benefits to them
  5. Duty to pay only reasonable and necessary plan expenses
  6. Duty not to engage in prohibited transactions
Act Prudently

• Prudent “Expert” Rule
  ◦ Discharge duties with the care, skill, prudence, and diligence that a prudent person acting in a like capacity would use in like circumstances

• Pure heart/empty head are not acceptable substitute for proper analysis

• Tip:
  ◦ Ask questions
  ◦ Discuss alternatives
  ◦ Challenge the status quo
  ◦ Seek expert advice if needed to make an informed choice
  ◦ Document process – inquiry, analysis, conclusion, and basis for conclusion
Use of Experts in Being Prudent

- Because the prudence rule requires the fiduciary to act with the care, skill, and prudence of one “familiar with such matters,” a fiduciary lacking the education, experience and skill required to make a decision has an affirmative duty to seek expert assistance.
  - The failure to do so violates the prudence standard.

- Prudence standard is not necessarily satisfied merely because the fiduciaries engage an appropriate expert and rely on the expert's advice.
  - Fiduciaries cannot rely on an expert's opinion unless:
    - They have investigated the expert's qualifications
    - Provided the expert with complete and accurate information and
    - Made certain that reliance on the expert's advice is reasonably justified under the circumstances
Procedural Prudence

• Procedural prudence involves three main requirements that fiduciaries must demonstrate:
  ◦ The details of the fiduciaries’ decision-making process
  ◦ That decisions are based on generally accepted investment/management practices
  ◦ That decisions are made in the best interest of participants
Fiduciary Functions

- Activities that give rise to fiduciary status include:
  - Being a plan sponsor - sometimes
  - Appointing other plan fiduciaries
  - Selecting and monitoring plan investment options
  - Selecting and monitoring third party service providers
  - Interpreting plan provisions
  - Exercising discretion in denying or approving benefit claims
  - Providing investment advice for a fee (limited exception for general education advice or use of qualified investment advisor)
Fiduciary Principles and Cybersecurity

- **Risk Assessment**: Recognize the risks to data
- **Duty of Loyalty**: Act in best interest of participants: adopt measures to manage the risks
- **Duty of Prudence**: Seek advice from experts
- **Hiring and Monitoring Service Providers**: Recognize risks when engaging third party service providers
Fiduciary Principles and Cybersecurity: Hiring and Monitoring Service Provider

• Selecting and Monitoring
  a) New considerations in light of cybersecurity
  b) Integrating new standards of evaluation
  c) Agreeing on reports to facilitate monitoring

• Contractual Considerations
  a) Representations that there is adequate cybersecurity structure
  b) Adequate insurance
  c) Indemnification
Fiduciary Principles and Cybersecurity: Hiring and Monitoring Service Providers

1. Does the service provider have a comprehensive and understandable cybersecurity program?

2. What are the elements of the service provider’s cybersecurity program?

3. How will the plan(s) data be maintained and protected?

4. Will the data be encrypted at rest, in transit and on devices, and is the encryption automated (rather than manual?)

5. Will the service provider assume liability for breaches?

6. Will the service provider stipulate to permitted uses and restrictions on data use?

7. What are the service provider’s protocols for notifying plan management in the case of a breach and are the protocols satisfactory?
Fiduciary Principles and Cybersecurity: 
Hiring and Monitoring Service Provider

8. Will the service provider agree to regular reports and monitoring and what will they include?

9. Does the service provider regularly submit to voluntary external reviews of their controls (such as SOC reports or a similar report or certification)?

10. What is the level and type of insurance coverage that is available?

11. What is the level of financial and fraud coverage that protects participants from financial damages?

12. If the service provider subcontracts to others, will the service provider insist on protections (as noted above) in its agreement with the subcontractor?

13. What controls does the service provider have in place over physical assets that store sensitive data, including when such assets are retired or replaced (servers, hard drives, mobile devices, etc.)?

14. What are the service provider’s hiring and training practices (for example, background checks and screening practices and cyber training of personnel)?
III. Cybersecurity – Fundamentals of a Successful Cybersecurity Plan

A. Assign ownership
B. Undertake thorough risk assessment
C. Adopt active, ongoing risk assessment plan
Cybersecurity – Fundamentals of a Successful Cybersecurity Plan: Ownership

1. Identify owner
2. Do they have adequate organizational resources to address cybersecurity?
3. Do they have institutional/organizational visibility?
4. Do they have adequate authority to implement a cybersecurity program?
5. Are they familiar with the benefit plans and service providers?
Cybersecurity – Fundamentals of a Successful Cybersecurity Plan: Risk Assessment

• What is a risk assessment?
  ◦ A factual finding, determine the risk to the data, and make recommendations

• Complete a risk assessment
  ◦ Risk assessment is an ongoing process
  ◦ Periodically re-evaluate protocols in response to environmental or operational changes affecting the security of data
  ◦ Periodically – every two or three years and whenever a new electronic technology is adopted or changed
Fundamentals of a Successful Cybersecurity Plan: Risk Assessment

- The risk assessment should include:
  - All information systems and servers
  - Laptops, smart phones, tablets
  - Mobile devices, wearables
  - Participant Portals
  - Cloud Storage Services
  - Social Media Presence
Cybersecurity Risk Management Strategy: Understanding Plan Data

- Thorough inventory of data utilized and shared as part of plan administration.
- How is the benefit plan data classified?
- Where is the benefit plan data stored?
- Who is accessing the benefit plan data?
- How is the benefit plan data accessed?
- Is access properly controlled?
- What are the threats?
Cybersecurity Risk Management Strategy: Principles for an Effective Plan

The cybersecurity risk management strategy cannot be a checklist.

- Instead – it must be dynamic, with commitment at highest levels, that includes:
  - Regular reporting
  - Frequent reviews
  - Process updates
Cybersecurity Risk Management Strategy: Process Considerations

- Implementation and Monitoring
- Testing and Updating
- Reporting
- Training
- Hiring Practices
- Controlling Access
- Data Retention and Destruction
- Third Party Risk Management
Cybersecurity Risk Management Strategy: Cybersecurity Frameworks

- Describe how to identify data risks
- Develop a program to protect data
- State how breaches will be detected
- Show how your plan can respond
- Detail how your plan will recover
Cybersecurity Risk Management Strategy: Customizing a Strategy

- Resources to Evaluate Cyber Risks
- Cyber Insurance
- New Developments
Cybersecurity Risk Management Strategy: Cyber Insurance Issues to Consider

- What limit of liability should be purchased?
  - Is it one aggregate limit or do separate limits of liability exist?
- What is the scope of coverage?
- How are claims handled?
- When and how should a claim be notified?
  - Don’t wait until you need it
  - Learn how to maximize and leverage the policy before you need it
Cybersecurity Risk Management Strategy: Cyber Liability Insurance

- Many plans are reluctant to buy it
  - Need for this insurance is not properly understood
- Other insurance policies do not fully respond
- Scope of cyber liability insurance, especially the first party services and coverages, is not properly understood
- Cost of a broad $1 - $2 million “safety net” policy is reasonable and competitive
Risk Management Strategy:
Cyber Liability Insurance

Reasons Given for Not Buying Cyber Liability Insurance

- It is not required
- It is too new
  - We have no evidence it will work and pay claims
- We have never had a claim
- We are not subject to HIPAA/HITECH
- We use a TPA
- We have strong security systems in place
- We have strengthened our vendor contracts
- It is too expensive
Takeaways

- Vulnerability of data in employee benefit plans coming into focus
- Standard cybersecurity policies and plans often miss this vulnerability
- Plan fiduciaries arguably have a duty to address plan participant data management
- A strong risk management plan requires:
  - Assigning ownership
  - Conducting thorough risk assessment
  - Building a risk management plan
Questions?
Reference Materials

- Summary of 2011 ERISA Advisory Council Recommendations
- Links to Materials
Best Practices from ERISA Advisory Committee 2011

Computers and Systems

A. Data
1. Keep only data that is needed.
2. Use effective processes to discard unnecessary data, including back-up paper and electronic copies.
3. Know where PII is located in all of the organization's systems.
4. Understand cloud computing and/or remote data storage, including how data is stored or protected.

B. Systems
1. Keep computer systems updated, including prompt installation of software patches.
2. Stay current on electronic threats and effective responses.
3. Follow National Institute of Security and Technology (NIST) guidelines on computer configuration.
4. Use full disk encryption on laptops and external data storage devices that might include PII or information on how to access it.
5. Maintain complete log-in for the network, firewalls, routers and key software applications.
6. Limit or define usage of portable devices.
Best Practices from ERISA Advisory Committee 2011

People and Training
1. Perform criminal background checks and drug screening for employees with access to PII.
2. Ensure all personnel who have access to PII are trained in properly safeguarding it. Include training in areas such as data retention/destruction, social networking, social engineering, and litigation holds.
3. Designate an individual to be in charge of privacy and security.
4. Educate all stakeholders regarding appropriate focus according to their roles.
5. Implement and test contingency plans for use in event of data breach.

Service Provider Management
1. Consider privacy and security factors regarding the selection and performing of due diligence for providers.
2. Make sure provider subcontractors are held to same standards as service provider.
Best Practices from ERISA Advisory Committee 2011

**General Tips**
1. Make sure to know what partners have access to PII and that they are paying attention to these issues.
2. Perform periodic risk assessments (Generally Accepted Privacy Principles)
3. Maintain good controls and be careful about who can over-ride them.
4. Use a process to confirm compliance with policies.
5. Make sure policies are clear and communicated to all appropriate parties.
6. Adopt a privacy policy designed for the organization.

**Special Concerns for Employees**
1. Educate employees about the importance of safe-guarding their data at all times.
2. Focus on security measures in place for distributions. Ensure added security for participants at time of distribution.
Additional Resources

- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- Vendor Security Assessment Questionnaire (VSAQ): https://vsaq-demo.withgoogle.com
- Office of Civil Rights (OCR): https://www.hhs.gov/hipaa/for-professionals
- OCR HIPAA Privacy Enforcement News: https://www.hhs.gov/hipaa/newsroom/index.html
- FBI Cyber Crimes: https://www.fbi.gov/investigate/cyber

**NOTE:** ERISA Advisory Council Reports from 2000 onward are available online at: https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/erisa-advisory-council/reports