United Actuarial Services, Inc.
Actuaries and Consultants

2017-24

April 19, 2017

CLIENT BULLETIN

Cybersecurity Considerations for Pension & Welfare Plans
Advice from the ERISA Advisory Council for Plan Sponsors

The Advisory Council on Employee Welfare and Pension Benefit Plans, generally referred to as the ERISA Advisory Council (the "Council") produced a report titled "*Cybersecurity Considerations for Benefit Plans*" ("Report"). The Council was established under Section 512 of *ERISA* to advise the Secretary of Labor on matters related to welfare and pension benefit plans. This 2016 cybersecurity report was produced for that purpose and builds on the 2011 Report.

The Goal of the Report

The *goal of the Report* was to educate and inform plan sponsors, fiduciaries and their service providers about the cybersecurity risks that they may face, existing frameworks that can form the foundation of a cybersecurity strategy, questions to ask and processes to consider establishing a cybersecurity strategy.

Although the contents of the Report do not represent the position of the Department of Labor, the Report contains valuable tips for sponsors of employee benefit plans, *including multiemployer pension and welfare plans*, among others. Every *ERISA*-governed employee benefit plan has confidential participant data it is required to protect. From the largest pension plan to the smallest vacation fund, employee benefit plans contain sensitive, personal, participant data which needs to be protected from unauthorized breaches.

In developing a robust cybersecurity program, Trustees will want to work closely with their IT vendor and other plan professionals.

What Data Are We Talking About?

We will adopt the Report's usage of the term "PII", short for "personally identifiable information". PII is broad enough to encompass the PHI ("protected health information") held by health plans which is already subject to the *HIPAA Privacy and Security Rules.* It would also encompass data held by pension plans and other

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: mewing@unitedactuarial.com

retirement plans, even though no overall federal data protection statute exists for such pension data as there is for data that is PHI.

In addition to benefit plans using confidential participant data, vendors to benefit plans often use and maintain plan participant data in the course of providing necessary services to employee benefit plans. As the Report also notes, "…*there continues to be no comprehensive federal law governing cybersecurity for benefit plan service providers*." Thus, the 2016 Report focuses on information that would be useful to plan sponsors, fiduciaries and their service providers in evaluating and developing a cybersecurity program to protect PII for these benefit plans. The main body of the Report contains discussions of some current cybersecurity frameworks that an employee benefit plan could adapt for its purposes.

Witnesses Outline Several Current Cybersecurity Dangers

The 2016 Council also heard witnesses report (click on the last blue bar titled "*2016 Written Statements By Invited Witnesses*") on the substantial threats in the environment in which benefit plans operate. Examples of cyber threats that were identified as common today include:

- *Ransomware* where criminals encrypt and seize an entire hard drive and will only release it for a high ransom. Various news sources reported that United Food and Commercial Workers (UFCW) Local 655 was the victim of a ransomware attack in July 2016, with one story including a copy of the notice letter.
- *Phishing* where fraudulent emails are sent with the objective of enticing the user to interact and inadvertently provide an avenue for a cyber-criminal to infiltrate a computer network.
- *Wire transfer email fraud* where cyber criminals pretend to be senior executives asking employees to transfer funds.
- *Malware via external devices* where intrusive and harmful software is stored on an external drive that is inserted into and executed on a network computer.

Cybersecurity and ERISA

The 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.

However, the Report also notes "*that 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 Report provides no answers to these questions as the 2016 Council determined that providing guidance on those topics was beyond the scope of its study.

Cybersecurity Tips for Plan Sponsors

In that light, the Report recommends that plan sponsors (the Board of Trustees in multiemployer benefit plans) *consider cybersecurity when making decisions to select or retain a service provider*. To aid in this task, Appendix A of the Report, "*Employee Benefit Plans: Considerations for Navigating Cybersecurity Risks*", includes helpful tips for addressing cybersecurity of employee benefit plans and their service providers. Below, we outline some topics discussed in Appendix A:

CYBERSECURITY RISK MANAGEMENT STRATEGY

UNDERSTANDING PLAN DATA
- How is the data classified?
- Where is the data stored?
- Who is accessing the data?
- How is data accessed?
- Is access properly controlled?
- What are the threats?

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

PROCESS CONSIDERATIONS
- Implementation and Monitoring
- Testing and Updating
- Reporting
- Training
- Hiring Practices
- Controlling Access
- Data Retention and Destruction
- Third Party Risk Management

CUSTOMIZING A STRATEGY
- Resources to Evaluate Cyber Risks
- Cyber Insurance
- New Developments
- Other Factors

Cybersecurity Tips and Contracting with Service Providers

Appendix A suggests that when contracting with service providers that use PII, such as third party administrators, pharmacy benefits managers, and record keepers, it may be helpful to ask the fourteen questions provided in the Appendix. We would also add other service providers to employee benefit plans to the list such as benefit consultants, investment advisors, actuaries, accountants and legal counsel, to name a few.

Trustees may wish to work with their plan professionals in customizing the cybersecurity questions asked of service providers. The Appendix suggests asking service providers that will be accessing and using the plan's PII the following questions:

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?
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 damage?
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)?

Conclusion

Cybersecurity is an increasing concern in all walks of life. A recent news item noted that a hacker gained access to the emergency siren system in Dallas and triggered all 156 of the city's emergency sirens around 11:40pm, setting off a wave of panic and confusion. With cyber dangers apparently lurking everywhere, Trustees need to regularly review and update their benefit plan's cybersecurity measures. This Report has helpful tips in addressing cybersecurity matters with plan service providers using PII, including PHI.

Additional Resources

- Appendix B of the Report at PDF page 37 contains a very helpful set of cybersecurity terms and definitions.

- Appendix C of the Report at PDF page 40 (last page) contains a number of useful links on cybersecurity, some of these and other links are listed below:

  - *NIST Cybersecurity Framework*: https://www.nist.gov/cyberframework
  - *Vendor Security Assessment Questionnaire (VSAQ):* https://vsaq-demo.withgoogle.com

- *National Conference of State Legislatures* list of state data breach and notice laws: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws
- *Health and Human Services Guidance on Ransomware:* http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- *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*

* * *