DOL Cybersecurity Guidance for Employee Benefit Plans

KATE FINLEY
Associate
Fisher Phillips

Email: kfinley@fisherphillips.com
Phone: (404) 240-5875

Agenda

- This year, the U.S. Department of Labor announced guidance for plan sponsors, plan fiduciaries, recordkeepers and plan participants on best practices for maintaining cybersecurity in benefit plans.
- With the exponential rise of cybersecurity incidents worldwide, it is critical that plans take precautions to mitigate the risk to sensitive plan information and plan assets.
- Central to these plans is identifying where threats can come from – internal and external – and how to best protect data at its weakest points.

Current Legal and Regulatory Data Privacy and Cybersecurity Landscape

- Group health plans (and business associates) must comply with HIPAA's provisions.
- Gramm-Leach-Bliley Act (Administered through SEC)
  - Requires financial institutions, such as investment advisory service providers, to safeguard sensitive data by developing administrative, technical, and physical safeguards to protect the confidentiality of consumer or customer data in their possession
  - Requirement to provide privacy notices to the financial institution's customers
- State Laws
  - States have adopted consumer protection laws and data breach notification laws
  - All states require consumer notification in the event of security breaches involving certain kinds of personal data (commonly SSNs)
  - ERISA preemption under the "relate to" prong is an open question with limited case law.

DATA PRIVACY AND SECURITY BASICS: At Risk Information

- Participant data, including Personally Identifiable Information, stored with a plan sponsor, third party service providers, or on the cloud is susceptible to breaches.
- Personally Identifiable Information has a broad definition
  - any information on a participant which can be used to determine an individual's identity (ex: name, social security number, etc.) alone, or when combined with other identifying information which is linked to that specific participant (such as date of birth, place of birth, mother's maiden name, etc.).

Retirement Plan Data Privacy And Security: Generally

- Data privacy and security issues are not new in the employee benefits context.
- Attacks on information systems maintained by plan sponsors and/or third-party service providers risks the possibility of identity theft and/or the theft or appropriation of retirement plan assets.
- Lawsuits have been brought against plans and trustees relating to distributions that were requested by unauthorized sources and insufficient processes and systems to detect the issues.

ERISA Fiduciary Considerations

- Protecting PII and other account data is not specifically enumerated as a fiduciary duty in ERISA, however, through recent guidance Department of Labor (DOL) has confirmed that plan fiduciaries have a duty to mitigate cybersecurity risks to their employer-sponsored plans.
- In addition, there is a general fiduciary duty under trust law to maintain confidentiality and privacy of third parties' information except as required by law or needed to administer the plan.
- The purchase of supplemental insurance policies covering cyber-related risks may not be necessary. However, doing so may fill gaps in existing processes and liability coverages and address expanded duties and potential liability.

DOL Cybersecurity Guidance for Employee Benefit Plans

- ERISA Advisory Council provided initial guidance in 2016 on suggested materials and considerations for plan sponsors, plan fiduciaries, and third-part service providers when developing cybersecurity strategies.
- Government Accountability Office urged the DOL to release guidance on cybersecurity matters in an effort to mitigate risks to 401(k) and other retirement plans.
- April 14, 2021 guidance: DOL did not issue statutory or regulatory guidance, but provided guidance focused on steps that should be taken by plan sponsors and fiduciaries, third-party service providers, and individuals.

DOL Cybersecurity Guidance for Employee Benefit Plans (cont'd)

- In issuing this guidance, the DOL recognized that plan fiduciaries have a duty to mitigate cybersecurity risks. The DOL's cybersecurity guidance was released in three parts:

1. Tips for Hiring a Service Provider with Strong Cybersecurity Practices, which provides guidance to plan fiduciaries in the hiring of service providers;

2. Cybersecurity Program Best Practices, which provides best practices for recordkeepers and other service providers; and

3. Online Security Tips, which provides advice to plan participants and beneficiaries who check and manage their accounts online.

Cybersecurity Program Best Practices

- In brief, the 12-point best practice system identified by the DOL is:

1. Have a formal, well-documented cybersecurity program. This includes a system to identify risks, protect assets, data and systems, detecting and responding to cybersecurity events, recovering from the event, disclosing events, and restoring normal operations and services. This program should be approved by senior leadership, reviewed internally at least annually, and should be reviewed by an independent third-party auditor to assess compliance and threats.

2. Create a prudent, annual risk assessment program. A manageable, effective risk assessment schedule should be established to assess cybersecurity risks and to describe how the program will mitigate identified risks. This program should be updated for changes.

Cybersecurity Program Best Practices (cont'd)

3. Engage a third-party annual audit of the security controls. An independent third-party auditor should assess the security controls on an annual basis and any corrections must be documented.

4. Clearly define and assign information security roles and responsibilities. Related to the first and second point, a prudent system to manage cybersecurity risks should clearly identify who has responsibility for each aspect of the program.

5. Ensure strong access control procedures. A strong procedure should be established to guarantee that users are who they say they are and that only approved users are able to access IT systems and data. This would require an appropriate system of authentication and authorization.

Cybersecurity Program Best Practices (cont'd)

6. Assess third-party service provider use of cloud computing. This would include requiring a risk assessment of the third-party service provider, periodically assessing the service provider, and ensuring that the guidelines of any safety program are satisfied.

7. Conduct annual cybersecurity awareness training. Conduct an annual cybersecurity awareness to at each level (including employees) to educate everyone to recognize attacks, help prevent incidents, and guard against identify theft.

8. Implement a secure system development life cycle (SDLC) program. A secure SDLC program ensures that security assurance activities, such as code review, are an integral part of the system development process.

Cybersecurity Program Best Practices (cont'd)

9. Implement a business resiliency program to address business continuity, disaster recovery, and incident response. Create a business continuity plan, disaster recovery plan, and an incident response plan.

10. Encrypt sensitive data. Implement current, prudent standards for encryption data that is stored and for data that is transmitted.

11. Implement strong technical controls to implement best security practices. Keep hardware, software, and firmware up to date, conduct routine data backup, and ensure routine patch management.

12. Be responsive to cybersecurity incidents or breaches. Ensure appropriate action is taken to protect the plan in the event of a cybersecurity incident or breach.

Tips for Hiring a Service Provider

- This guidance now sweeps cybersecurity considerations into the topics of consideration when selecting service providers.
- The DOL provides suggested questions to ask potential service providers in order to gauge that service provider's cybersecurity practices. This includes asking the service provider about:
  - their information security standards,
  - audit policies and results,
  - how it validates its practices,
  - what levels of security standards it has met and implemented, and past security breaches.

  The responses should be considered against other potential service providers, industry standards, and the service providers track record.

Tips for Hiring a Service Provider

- Guidance on the actual review and negotiation process for hiring service providers and considerations in monitoring and assessing the relationship. Contracts should:
  - Require the service provider to obtain third-party audits on an annual basis;
  - Specify the service provider's obligation to keep private information private, prevent disclosure, and meet a strong standard of care to do so;
  - Identify how quickly a service provider must inform plan fiduciaries of breaches;
  - Specify the service provider's obligation to meet applicable federal, state, and local laws regarding privacy, confidentiality, or security of participant's personal information;
  - Include a broad definition of "data security breach" so that it includes "suspected breaches; and
  - Generally, clarify the roles of responsibilities of the vendor and the plan fiduciaries.

Online Security Tips

- The final component of the DOL guidance focuses on steps and actions that plan participants and beneficiaries can take to mitigate potential cybersecurity risks on their end.

- These tips include regular monitoring of their accounts, the use of strong passwords with multi-factor authentication, updating personal contact information, and signing up for account activity notices.

Online Security Tips

- As part of this advice, the DOL also provides individuals with some general best practice considerations when accessing accounts or having an online presence generally, such as:
  - Routinely monitoring their online account;
  - Using strong and unique passwords;
  - Using multi-factor authentication;
  - Keeping personal information current;
  - Being careful with public wi-fi;
  - Being award of phishing and spoofing attacks; and
  - Using up to date antivirus software and applications.

Moving Forward with the DOL Guidance: Generally

- Establish, if you have not already, a cybersecurity procedure.
  - May require expanding an existing program/procedure to cover or include benefit plans or otherwise broadening an existing program.
- Review current service provider contracts and hiring processes, particularly for any contracts that are coming up for renewal.
- Adopt an internal procedure to document compliance with the DOL guidance.

Moving Forward with the DOL Guidance: Audits

- DOL guidance has only been available for a few months and is not in the form of formal statutes or regulatory requirements with associated penalties, but audits have already begun to include cybersecurity issues.
- DOL has supplemented existing audits with cybersecurity information and document requests and newly commenced audits are including similar requests.

Final Questions

Email: ubamember@fisherphillips.com

HRCI –

SHRM –

KATE FINLEY
Associate
Fisher Phillips

Email: kfinley@fisherphillips.com
Phone: (404) 240-5875

Thank You

KATE FINLEY
Associate
Fisher Phillips

Email: kfinley@fisherphillips.com
Phone: (404) 240-5875