Do You Have an Employee Benefit Plans' Cybersecurity Policy?

The Department of Labor Wants to Know

By:Rebecca F. Alperin
January 24, 2023

Cybersecurity Responsibilities of ERISA Plans

Did you know that ERISA plan fiduciaries have a duty to mitigate risks of malfeasance to plans posed by internal and external cybersecurity threats? This makes sense as ERISA-covered plans contain millions of dollars in assets and pertinent participant personal data. Fortunately, in April 2021, the Department of Labor ("DOL") issued a cybersecurity guidance package which sets forth best practices for plan fiduciaries to reduce cybersecurity risks associated with employee benefit plans. Keep in mind that these guidelines are in addition to HIPAA data security requirements applicable to group health plans. We urge you to be prepared, because when the DOL comes knocking on audit, it likely will ask to see all documents substantiating any cybersecurity or information security programs that apply to a plan's data, whether those programs are applied by the plan sponsor or by any service provider to the plan.

It is not too late to take action. Action items for plan fiduciaries and sponsors include:

- Review the guidance.
- Assess how current cybersecurity practices and those of recordkeepers and service providers compare with the DOL best practices.
- Develop a plan to implement the recommendations.
- Conduct fiduciary training as part of any cybersecurity program.
- Amend service provider contracts and plan documents as appropriate.

Importantly, fiduciaries, sponsors, recordkeepers, and service providers should document compliance efforts. The DOL and other regulators will expect ERISA plan sponsors and fiduciaries to substantiate their cybersecurity compliance training, procedures, and participant disclosure approaches. On audit, actions will speak louder than words. It may not be enough to say, "we are doing this," or "we have implemented antivirus and firewalls to protect our information systems." Be prepared to demonstrate that one or more of the following have been implemented or adopted:

- The implementation of access controls and identity management, including any use of multi-factor authentication.
- The processes for business continuity, disaster recovery, and incident response.
- Management of vendors and third-party service providers, including notification protocols for cybersecurity events and prohibiting the use of data for any purpose other than the direct performance of their duties.
- Cybersecurity awareness training.

- Encryption to protect all sensitive information transmitted, stored, or in transit.
- Annually, engage a reliable third-party audit of security controls.

Similarly, fiduciaries should adopt protocols which incorporate the "six factors for plan sponsors to consider when selecting ERISA plan service providers" outlined in the DOL's cybersecurity guidance package and be prepared to produce all documents and communications from service providers relating to their cybersecurity capabilities and procedures. To reiterate, existing service provider agreements may need to be amended so that plan fiduciaries can demonstrate compliance with the DOL's guidelines.

Cybersecurity is a new and important area of interest for the DOL and plan fiduciaries need to be prepared to respond. The best practices and tip sheets outlined by the DOL should be considered by all organizations regardless of the size of the plan assets and participants.

If you have questions about the applicability of the DOL guidance and your regulatory obligations related to cybersecurity responsibilities of ERISA plans, please contact Rebecca Alperin or any member of our Privacy & Data Security Team.