SpencerFane®

Cybersecurity for Benefit Plans

In 2021, the U.S. Department of Labor (DOL) issued cybersecurity guidance for retirement plans. That guidance included:

- Cybersecurity Program Best Practices;
- Tips for Hiring Service Providers with Strong Cybersecurity Programs; and
- Online Security Tips.

In October 2024, the DOL updated its guidance and confirmed its applicability to all employee benefit plans, including health and welfare plans.

Cybersecurity Program Best Practices

The DOL's Cybersecurity Program Best Practices highlights the duty imposed on plan fiduciaries to limit risk to plan data, assets, and participant information. It states,

ERISA-covered pension plans and health and welfare plans often hold millions of dollars or more in assets. Additionally, pension, health, and welfare plans store and/or transfer participant personally identifiable data, which can make them tempting targets for cybercriminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

What's a Plan Fiduciary to do?

Be Prepared. Plan fiduciaries should work with their legal counsel and benefits consultants to review and apply the DOL guidance and develop practical tools to satisfy the measures recommended by the DOL, including a documented cybersecurity program, annual risk assessments, defined roles and responsibilities, and robust access control and data storage measures.

Assess and Monitor Vendors. Many plan fiduciaries rely heavily on third-party vendors and contracted service providers to administer the plan's eligibility rules, benefits, and plan assets. Fiduciaries have a duty to assess and monitor the cybersecurity of such vendors. Questionnaires and a thorough analysis of vendor responses can shed light on vendors' cybersecurity systems and help plan fiduciaries identify potential risks.

Cybersecurity Training. The DOL recommends annual cybersecurity awareness training among its best practices. Plan fiduciaries and key employees should undertake regular training and ensure the plan's vendors and service providers do the same. Plan-specific training can help fiduciaries identify necessary action steps to shore up their security measures and monitor vendors that have access to plan data, assets, and participant information.

Be Responsive. Even the best prepared and trained fiduciaries and benefit plans can experience breaches or cyber incidents. Plan fiduciaries should know who to contact to mitigate the plan's risk. Responsiveness also requires notification to the plan's cyber liability insurer and other parties, including participants, contractors, and law enforcement.

Utilize Legal Counsel

Spencer Fane can help your plan be prepared and responsive with plan-specific cybersecurity training and other tools for monitoring vendors, assessing risk, and creating strong practices.

This blog was drafted by Laura Fischer, an attorney in the Spencer Fane Denver, Colorado, office and Shawn Tuma, an attorney in the Spencer Fane Plano, Texas office and the leader of the firm's Cyber | Data | Artificial Intelligence | Emerging Technology team. For more information, visit www.spencerfane.com.

Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.