09/11/24 Employee Benefits Compliance

Key Cybersecurity Guidance Applicable to Group Health Plans and Fiduciaries

Background

In April 2021, the Department of Labor's (DOL) Employee Benefits Security Administration (EBSA) issued guidance on cybersecurity best practices for plan sponsors, fiduciaries, service providers, and participants to safeguard plan data, personal information and, where applicable, plan assets. At the time the guidance was issued, stakeholders and practitioners generally concluded that it was applicable only to retirement plans. On September 6, 2024, the EBSA issued Compliance Assistance Release No. 2024-01 (Release No. 2024-01) specifically stating that the 2021 cybersecurity guidance is applicable to all employee benefit plans, including health and welfare plans. This includes medical, dental, and vision plans as well as plans that provide life and AD&D insurance, most health flexible spending arrangements, health reimbursement arrangements, and other benefit plans covered by ERISA. As a result, group health plan sponsors should closely review this guidance and incorporate it into their overall ERISA fiduciary compliance, especially as it relates to evaluating plan service providers. Note that while benefits professionals should be familiar with this guidance, engagement from IT professionals in the organization is crucial. Cybersecurity practices have been a new and recent focus of DOL health and welfare plan audits, so it is important for plan sponsors of all sizes and types to be familiar with the DOL's expectations here. We provide an overview of the key components of the guidance below.

Cybersecurity Guidance for Health and Welfare Plan Fiduciary Compliance

Release No. 2024-01 confirms the application of this guidance to group health plans and includes three separate documents for plan sponsors and plan fiduciaries to review and consider related to cybersecurity and compliance with their fiduciary duties. Perhaps most notable is the impact on the fiduciary duty of prudence, which is specifically referenced in these materials. The three pieces are outlined below.

- **Tips for Hiring a Service Provider**. This piece is largely directed at plan sponsors and plan fiduciaries. The EBSA notes that this piece is intended to help employers and other plan sponsors and plan fiduciaries "meet their responsibilities under ERISA to *prudently select* and monitor" service providers" and includes specific recommendations set forth below. Note that a robust vendor management process will likely support compliance on most of these recommendations:
    - Ask about the service providers' information security standards, practices and policies, and audit results and compare them to industry standards.
    - Ask how the service provider validates its practices and what levels of security standards it has met and implemented. Look for contractual provisions that give the plan sponsor the right to audit cybersecurity practices.
    - Evaluate the service provider's track record in the industry, including litigation and security incidents.
    - Ask about prior security breaches and responses.
    - Inquire about the service providers cybersecurity liability insurance.
    - Ensure contracts require service provider ongoing compliance with cybersecurity and data security standards. Include terms in the contract that enhance cybersecurity for the plan and its participants.

- **Cybersecurity Program Best Practices**. Here, the EBSA notes that responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks and outlines 12 best practice approaches for plan service providers responsible for plan-related IT systems and data, and for plan fiduciaries *making prudent decisions* on the service providers they should hire. For a group health plan, those service providers could include, but are not limited to, any third-party administrator (TPA) handling plan data or processing claims, benefits administration systems, data analytic warehouses holding data on behalf of the plan, point solution vendors such as targeted disease management, telemedicine, or primary care vendors. Notably, the EBSA calls for a plan sponsor's cybersecurity program to be managed at the executive level, ideally by the Chief Information Security Officer (CISO). This guidance is robust and technical, and both the benefits and IT professionals in an organization should review it closely. In summary, it recommends that service providers should have a formal, well-documented cybersecurity program, conduct annual risk assessments, undertake third party audit of security controls, clearly define and assign information security roles, have strong access control procedures, ensure any assets or data stored in a cloud or by a third party service provider are subject to security reviews and independent security assessments, conduct periodic (at least annually) security awareness training, implement and manage a secure system development life cycle (SDLC) program, have an effective business continuity/disaster recovery program, encrypt sensitive data stored and in transit, implement strong technical controls according to best security practices, and appropriate responses to past security incidents.

- **Online Security Tips**. This guidance is directed at participants and includes a list of fairly intuitive best practices to reduce the risk of fraud and cybersecurity threats to plan-related information including, but not limited to, using multifactor authentication, routinely monitoring accounts and updating passwords, avoiding free Wi-Fi, keeping personal contact information current, and closing or deleting unused accounts. Although not a requirement, plan sponsors may want to consider including this information in plan-related materials and can use this EBSA piece for that purpose.

Takeaways

Given that DOL officials have publicly stated an intention to focus on cybersecurity issues in its ERISA investigations this cybersecurity guidance is a key part of a plan fiduciary's overall ERISA fiduciary compliance, and requires active engagement not only from benefits professionals, but also IT professionals within an organization. This guidance includes specific recommendations and action items that plan sponsors should review against their current policies and procedures. A robust vendor management program, increasingly common at least in larger organizations, will often have already implemented many of these best practice recommendations and/or can be the key mechanism by which a plan sponsor implements these best practices. Plan sponsors should also work with their outside counsel and advisors to ensure this guidance is incorporated into the overall plan decision making process as necessary to comply with their ERISA fiduciary duties. Contact your Alliant representative for more information on Alliant's approach here, including the availability of our ERISA Fiduciary Toolkit.