Published on *The National Law Review* https://natlawreview.com

# DOL Expands Fiduciary Obligations for Cybersecurity to Health and Welfare Plans

Article By:

Joseph J. Lazzarotti

A little more than three years ago, the U.S. Department of Labor (DOL) posted cybersecurity guidance on its website for ERISA plan fiduciaries. That guidance extended only to ERISA-covered retirement plans, despite health and welfare plans facing similar risks to participant data.

Last Friday, the DOL's Employee Benefits Security Administration (EBSA) issued Compliance Assistance Release No. 2024-01. The EBSA's purpose for the guidance was simple – confirm that the agency's 2021 guidance generally applies to **all** ERISA-covered employee benefit plans, including health and welfare plans. In doing so, EBSA reiterated its view of the expanding role for ERISA plan fiduciaries relating to protecting plan data:

***"Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.***"

In 2021, we outlined the DOL's requirements for plan fiduciaries here, and in a subsequent post discussed DOL audit activity that followed shortly after the DOL issued its newly minted cybersecurity requirements.

As noted in our initial post, the EBSA's best practices included:

- *Maintain a formal, well documented cybersecurity program.*
- *Conduct prudent annual risk assessments.*
- *Implement a reliable annual third-party audit of security controls.*
- *Follow strong access control procedures.*
- *Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.*
- *Conduct periodic cybersecurity awareness training.*
- *Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.*
- *Encrypt sensitive data, stored and in transit.*

Indeed, the substance of the guidance is largely the same, as indicated above, and still covers three areas – Tips for Hiring a Service Provider, Cybersecurity Program Best Practices, and Online

Security Tips (for plan participants). What is different are some of the issues raised by the new plans to which the expanded guidance applies – health and welfare plans. Here are some examples.

- **The plans covered by the DOL's guidance**. As noted, the DOL's cybersecurity guidance now extends to health and welfare plans. This includes plans such as medical, dental, and vision plans. It also includes other familiar benefit plans for employees, including plans that provide life and AD&D insurance, LTD benefits, business travel insurance, certain employee assistance programs and wellness programs, most health flexible spending arrangements, health reimbursement arrangements, and other benefit plans covered by ERISA. Recall that an "employee welfare benefit plan" under ERISA generally includes:

*"any plan, fund, or program…established or maintained by an employer or by an employee organization…for the purpose of providing for its participants or their beneficiaries, through the purchase of insurance or otherwise…medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, death or unemployment, or vacation benefits, apprenticeship or other training programs, or day care centers, scholarship funds, or prepaid legal services.*"

A threshold compliance step for ERISA fiduciaries, therefore, will be to identify the plans in scope. However, cybersecurity should be a significant compliance concern for just about any benefit offered to employees, whether covered by ERISA or not.

- **Identifying service providers**. It is tempting to focus on a plan's most prominent service providers – the insurance carrier, claims administrator, etc. However, the DOL's guidance extends to all service providers, such as brokers, consultants, auditors, actuaries, wellness providers, concierge services, cloud storage companies, etc. Fiduciaries will need to identify what individuals and/or entities are providing services to the plan.
- **Understanding the features of plan administration.** The nature and extent of plan administration for retirement plans as compared to health and welfare plans often is significantly different, despite both being covered by ERISA which includes a similar set of compliance requirements. For instance, retirement plans tend to collect personal information only about the employee, although there may be a beneficiary or two. However, health and welfare plans, particularly medical plans, often cover an employee's spouse and dependents. Additionally, for many companies, different groups of employees monitor retirement plans versus health and welfare plans. And, of course, more often than not, there are different vendors servicing these categories employee benefit plans.
- **What about HIPAA?** Since 2003, certain group health plans have had to comply with the privacy and security regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The DOL's cybersecurity guidance, however, raises several distinct issues. First, the DOL's recent pronouncements concerning cybersecurity are directed at fiduciaries, who as a result may need to take a more active role in compliance efforts. Second, obligations under the DOL's guidance are not limited to group health plans or plans that reimburse the cost of health care. As noted above, popular benefits for employees such as life and disability benefits are covered by the DOL cybersecurity rule, not HIPAA. Third, the DOL guidance appears to require greater oversight and monitoring of plan service providers than HIPAA requires of business associates. In several places, the Office of Civil Rights' guidance for HIPAA compliance states that covered entities are not required to monitor a business associate's HIPAA compliance. See, e.g., here and here.

The EBSA's Compliance Assistance Release No. 2024-01 significantly expands the scope of compliance for ERISA fiduciaries with respect to their employee benefit plans and cybersecurity, and

by extension the service providers to those plans. Third-party plan service providers and plan fiduciaries should begin taking reasonable and prudent steps to implement safeguards that will adequately protect plan data. EBSA's guidance should help the responsible parties get there, along with the plan fiduciaries and plan sponsors' trusted counsel and other advisors.



National Law Review, Volume XIV, Number 253