Legal Update

Brought to you by: Evolution of Benefits

EBSA Releases Updated Cybersecurity Guidance for Employee Benefit Plans

Through Compliance Assistance Release No. 2024-01, the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) is confirming that the cybersecurity guidance it issued in April 2021 generally applies to all employee benefit plans, including health and welfare plans.

Background

In 2021, EBSA issued cybersecurity guidance to help plan sponsors, fiduciaries, service providers, and participants in employee benefit plans safeguard plan data, personal information and plan assets. However, in the years since, health and welfare plan service providers have told fiduciaries and EBSA investigators that this guidance only applies to retirement plans. Thus, it was recommended in 2022 that EBSA clarify that the guidance also applies to health benefit plans.

Updated Guidance

The Compliance Release clarifies that the cybersecurity guidance applies to all types of plans covered by the Employee Retirement Income Security Act of 1974 (ERISA), including health and welfare plans and all employee pension benefit plans. EBSA is providing the following updated guidance:

1. **Tips for Hiring a Service Provider**: This guidance helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as required by ERISA.
2. **Cybersecurity Program Best Practices**: This guidance assists plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks.
3. **Online Security Tips**: This guidance offers plan participants and beneficiaries who check their retirement accounts or other employee benefit information online basic rules to reduce the risk of fraud and loss.

Additional Resources

The U.S. Department of Health and Human Services also offers publications that may help health plans and their service providers maintain good cybersecurity practices, as follows:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations

evolution of benefits
. . . bringing employee benefits full circle

ERISA Fiduciary Obligations

Plan fiduciaries of ERISA-covered pension plans and health and welfare plans have an obligation to ensure proper mitigation of cybersecurity risks.

Employers and other sponsors of health, welfare, 401(k) and other types of pension plans often rely on service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.