

Compliance Assistance Release No. 2024-01

Cybersecurity Guidance Update

U.S. Department of Labor
Employee Benefits Security Administration
September 6, 2024

I. Purpose

The Employee Benefits Security Administration (EBSA) is confirming that the cybersecurity guidance issued by EBSA in April 2021 generally applies to all employee benefit plans, including health and welfare plans.

II. 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. The Department of Labor's ERISA Advisory Council recommended in 2022 that EBSA clarify that the guidance also applies to health benefit plans.

III. Update

Through this Compliance Assistance Release, we clarify that the cybersecurity guidance applies to all types of ERISA plans, including health and welfare plans and all employee pension benefit plans. This is reflected in the updated guidance below:

- [Tips for Hiring a Service Provider](#): Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.
- [Cybersecurity Program Best Practices](#): Assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks.
- [Online Security Tips](#): Offers plan participants and beneficiaries who check their retirement accounts or other employee benefit plan information online basic rules to reduce the risk of fraud and loss.

The Department of Health and Human Services also offers publications that may help health plans and their service providers maintain good cybersecurity practices.

- [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