

# DOL Confirms Cybersecurity Guidance Applies to All Employee Benefit Plans

---

*September 23, 2024*

The U.S. Department of Labor (DOL) published [Compliance Assistance Release No. 2024-01](#) on September 6, 2024. The release, titled “Cybersecurity Guidance Update,” clarifies that the cybersecurity guidance the DOL issued in April 2021 applies to all employee benefit plans, including health and welfare plans. The DOL states that since the guidance was published, service providers have told plan fiduciaries and Employee Benefits Security Administration (EBSA) investigators that the guidance applies only to retirement plans.

The 2021 guidance consists of three parts: (1) [Tips for Hiring a Service Provider](#) (directed toward plan sponsors and fiduciaries), (2) [Cybersecurity Program Best Practices](#) (directed toward recordkeepers and other service providers responsible for plan-related IT systems and data), and (3) [Online Security Tips](#) (directed toward plan participants and beneficiaries). To further clarify that the guidance applies to all plans, the DOL updated each of the three parts to specify that plan participants, employers, plan sponsors and fiduciaries of both retirement *and* health and welfare plans should follow the guidance contained in each part and maintain strong cybersecurity practices.

The DOL also pointed health and welfare plan sponsors toward the following cybersecurity guidance published by the U.S. Department of Health and Human Services:

- [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

## ***Considerations for Plan Sponsors and Other Fiduciaries***

See our previous [Update](#) on the DOL's cybersecurity guidance for a more detailed summary of best practices and considerations. In general, the guidance indicates plan sponsors and fiduciaries should do the following:

1. Select and monitor service providers with an eye towards cybersecurity.
2. Conduct periodic reviews of the cybersecurity programs of recordkeepers and other service providers.
3. Review the terms of agreements with service providers to ensure they contain best practice

provisions and require ongoing compliance by the service provider with cybersecurity and information security standards.

4. Educate participants and beneficiaries who manage their benefit accounts online about online security.

In the updated guidance, the DOL added the following additional guidelines:

- In the Tips for Hiring a Service Provider, the DOL indicated that the plan fiduciary should find out if the service provider has any insurance that would cover losses caused by cybersecurity and identity theft breaches.
- In the Cybersecurity Program Best Practices, the DOL added additional detail on multifactor authentication (MFA), including that service providers should deploy phishing-resistant MFA if possible, implement MFA on internet-facing systems, and require MFA to access areas of the service provider's networks containing sensitive information.
- In the Online Security Tips, the DOL advised that participants should use longer passwords, not common passwords, and change their longer passwords only annually instead of more frequently.

Plan sponsors and fiduciaries should keep DOL's guidance in mind as they assess their cybersecurity programs. In particular, the DOL's guidance is a good reminder to consider their health and welfare plans' data flows, systems, and vendors in cybersecurity risk assessments and reviews to help implement best practices and strategies to mitigate cybersecurity risks.

## CONTACTS

If you have any questions regarding how the updated DOL cybersecurity guidance affects your employee benefit plan, please contact the Sidley lawyer with whom you usually work, or

<b>Colleen Theresa Brown</b> , Partner	+1 202 736 8465, <a href="mailto:ctbrown@sidley.com">ctbrown@sidley.com</a>
<b>Beth J. Dickstein</b> , Partner	+1 312 853 6093, <a href="mailto:bdickstein@sidley.com">bdickstein@sidley.com</a>
<b>Mary C. Niehaus</b> , Partner	+1 312 853 6090, <a href="mailto:mniehaus@sidley.com">mniehaus@sidley.com</a>
<b>Madeline Clasen</b> , Associate	+1 312 853 7776, <a href="mailto:mclasen@sidley.com">mclasen@sidley.com</a>

---

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at [www.sidley.com/en/locations/offices](http://www.sidley.com/en/locations/offices).

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at [www.sidley.com/disclaimer](http://www.sidley.com/disclaimer).

© Sidley Austin LLP