Verrill

DOL Updates Cybersecurity Guidance for ERISA Plans

by Karen K. Hartford on December 18, 2024

On September 6, 2024, the U.S. Department of Labor (DOL) issued a press release announcing that it was publishing updated cybersecurity guidance in the form of Compliance Assistance Release No. 2024-01 for all plans governed by the Employee Retirement Income Security Act of 1974 (ERISA). The new guidance updates the DOL's April 2021 cybersecurity guidance, which we summarized in a June 23, 2021 blog post. While the changes to the 2021 guidance were few, they clarify that the DOL's guidance applies not only to ERISA-governed retirement plans but also to ERISA-governed health and welfare plans. The updated guidance also offers new advice about analyzing health and welfare vendor cybersecurity practices, vendor insurance coverage, multi-factor authentication, and the importance of swift participant breach notification.

Like the 2021 guidance, the DOL's 2024 guidance is composed of three documents: (1) *Tips for Hiring a Service Provider with Strong Cybersecurity Practices*, which offers advice to plan sponsors and fiduciaries regarding the selection of vendors with strong and compliant cybersecurity practices and monitoring vendor activities; (2) *Cybersecurity Program Best Practices*, which supports plan fiduciaries and third party administrators seeking to mitigate cybersecurity risk in general; and (3) *Online Security Tips,* which offers advice to plan participants about what they can do to protect themselves and their benefit accounts online. The updated guidance changed only documents (1) and (2) above, which are explained in the remainder of this post.

What's New

Tips for Hiring a Service Provider with Strong Cybersecurity Practices: First, the guidance has been updated to state clearly that it applies to all types of ERISA-governed employee benefits plans. While the 2021 guidance was styled to apply to retirement plans, the updated guidance explicitly names health and welfare plans and notes that the guidance applies to plans of all types and sizes.

Following from this, the guidance has been revised to advise that employers and other plan sponsors and plan fiduciaries should be asking their health and welfare plan service providers about their security standards, practices and policies, and audit results and then

comparing their responses to the industry standards adopted by other vendors providing comparable services. The guidance further states that plan fiduciaries should be looking for service providers that follow a recognized information security standard and use an outside, third-party auditor to review and validate their cybersecurity practices, preferably annually.

Last, the DOL updated the guidance to emphasize that when employers, other plan sponsors, and plan fiduciaries ask vendors about their insurance coverage, they should be sure to request enough information to ensure that they understand not only the terms and limits of the coverage but also to confirm that the policy covers losses related to cybersecurity breaches and incidents involving their clients' benefit plans specifically.

Cybersecurity Program Best Practices: The guidance was updated to reference health and welfare plans. It also added a note to remind plan fiduciaries that ERISA plans "store and/or transfer participant personally identifiable data, which can make them tempting targets for cybercriminals."

In Section 5, regarding access control procedures, the updated guidance has doubled down on using multi-factor authentication (MFA). MFA is an account log-in process that requires multiple methods of proving that the user is who they say they are (for example, combining a password entry with a unique code notification pushed to the user's phone). The 2021 guidance encouraged the use of MFA wherever possible. The new guidance calls for the use of "phishing-resistant" MFA (for example, a password combined with facial or other biometric recognition) wherever possible; the implementation of MFA on Internet-facing systems, rather than in-house systems only; and requiring MFA to access any areas of a network with sensitive, private information, such as HIPAA-protected health information.

In Section 12, regarding responsiveness to cybersecurity incidents or breaches, the new guidance adds that when a cybersecurity breach or incident occurs, not only should law enforcement and insurers be notified, but participants should be notified of the breach of their personal data without unreasonable delay.

Last, *Cybersecurity Program Best Practices* was updated to provide an "Additional Resources" section, including links to documents published by the Department of Health and Human Services relating to cybersecurity practices in the health industry and within healthcare organizations and a document published by the Cybersecurity & Infrastructure Security Agency about implementing phishing-resistant MFA.

There's A Lot at Stake

Health and welfare plans and the healthcare industry as a whole hold a treasure trove of sensitive information for cybercriminals—from private, health-related information to demographic information and social security numbers to credit card and other financial information. The DOL's September press release describes the magnitude of the issues:

> "...as of June 2024, EBSA estimates ERISA covers 2.8 million health plans, 619,000 other welfare benefit plans and 765,000 private pension plans in America. These plans include 153 million workers, retirees and dependents who participate in private sector pension and welfare plans with $14 trillion in estimated assets. Without sufficient protections, digital participant and assets information may be vulnerable to the internal and external risks of computer-related crimes and losses. Federal regulations require plan fiduciaries to take appropriate precautions to mitigate these risks."

In short, the stakes are high, and the fallout can be far-reaching. Cybersecurity is not a matter to be left to chance. Moreover, the DOL's September press release makes clear that the Employee Benefits Security Administration considers cybersecurity for *all* types of ERISA plans to be "a great concern," and it will continue to investigate cybersecurity issues and make enforcement a priority.

If you have questions about mitigating the risks of cybersecurity violations for your ERISA plans, please contact any member of Verrill's Employee Benefits and Executive Compensation practice group.

Karen K. Hartford
Partner
T (207) 253 4910
email