Issued date: 10/16/24

Cybersecurity Guidance Applies to Health and Welfare Benefits

The Employee Benefits Security Administration ("EBSA") of the U.S. Department of Labor confirmed in Compliance Assistance Release No. 2024-01 that cybersecurity guidance issued in 2021 applies to all ERISA-covered health and welfare plans. This guidance goes beyond what is required under HIPAA for health plans, and includes "Tips for Hiring a Service Provider," "Cybersecurity Program Best Practices," and "Online Security Tips," which were updated to reflect this clarification.

Background

In April 2021, EBSA issued cybersecurity guidance for benefit plan fiduciaries and service providers, regarding best practices for maintaining cybersecurity. Recognizing that ERISA requires plan fiduciaries to take appropriate precautions to mitigate cybersecurity risks, EBSA's guidance came in three forms, directed at benefit plan sponsors, fiduciaries, record keepers, and participants.

The language in the original guidance led to confusion as to whether the guidance applied solely to retirement plans. With this new guidance, EBSA clarifies that its cybersecurity guidance does, in fact, also apply to ERISA-covered health and welfare plans.

Details of the Guidance

Cybercrime is a constant and growing risk across the globe, and employer-based benefit plans have not escaped falling victim to these crimes. Health and welfare benefit plans carry some risk of financial loss to plan sponsors and participants, but they generally carry significantly more risk of disclosure of personally identifiable information ("PII") and sensitive health information of plan members, as well as their covered family members, over multiple benefits and across multiple service providers.

The Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") is designed to, among other things, impose extensive privacy and security requirements to employer-provided group health plans to secure protected health information ("PHI") and electronic PHI secure. Plan sponsors, fiduciaries, and business associates of group health plans, such as third-party administrators ("TPAs"), who take significant steps in ensuring compliance with HIPAA, will have already made

strides in complying with EBSA's ERISA cybersecurity guidance. However, it is important to note that various ERISA-covered welfare benefits are not group health plans subject to HIPAA, including group-term life insurance, disability coverage, and accident-only coverage. Such benefits would generally be subject to ERISA and to which the EBSA cybersecurity guidance would apply.

Both the original 2021 guidance and the recent guidance provide links to three separate pieces. The first two are oriented towards plan fiduciaries and service providers, and the degree to which fiduciaries adopt the detailed suggestions may depend on the size and complexity of their plans, particularly the amount of plan assets and data that they may handle.

Tips for Hiring a Service Provider

EBSA provides six tips directed at a plan fiduciary as recommendations to support prudent selection and monitoring of service providers and recommends requesting the following information:

1. information on the service provider's cybersecurity standards and compare against recognized industry standards. Perhaps involve internal IT experts.
2. how provider validates practices.
3. provider's track record, including third party reports on the provider.
4. providers' prior experience with breaches.
5. information on insurance policies covering cybersecurity losses and identity theft breaches.
6. contract terms (to watch for and consider):
    a. attempts to limit service provider's responsibilities;
    b. service provider ideally obtaining annual third-party audit for compliance;
    c. high standards by provider to secure information;
    d. notify plan fiduciary of incidents/breaches promptly and to properly address;
    e. oblige provider to follow all laws (e.g., retention and destruction of information); and
    f. require insurance.

Health and welfare plan fiduciaries should keep these suggestions in mind for all plan service providers. Though this would mainly pertain to an insurer, TPA, or PBM, it extends to consultants, wellness vendors, data analysts, trustees, etc. as well.

Cybersecurity Program Best Practices – Service Provider

EBSA provides a highly detailed summary of best practices for ERISA plan services providers cybersecurity program. Health and welfare benefit plan fiduciaries may also use this piece to evaluate the extent to which such providers are applying best practices. There are twelve different recommendations, including:

1. having a formal, well documented cybersecurity program
2. conducting prudent annual risk assessments
3. having a reliable annual third-party audit of security controls
4. clearly defining and assigning information security roles and responsibilities
5. having strong access control procedures
6. ensuring 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.
7. conducting periodic cybersecurity awareness training.
8. implementing and managing a secure system development life cycle ("SDLC") program.
9. having an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. encrypting sensitive data, stored and in transit.
11. implementing strong technical controls in accordance with best security practices.
12. appropriately responding to any past cybersecurity incidents.

Online Security Tips

Lastly, the EBSA guidance provides 9 basic rules oriented to plan members when they are accessing online health, welfare, or retirement accounts, specifically:

1. register, set up and routinely monitor your online account.
2. use strong and unique passwords/passphrases.
3. use Multi-Factor Authentication.
4. keep personal contact information current.
5. close or delete unused accounts.
6. be wary of free Wi-Fi.
7. beware of phishing attacks.
8. use antivirus software and keep apps and software current.
9. know how to report identity theft and cybersecurity incidents.

Employer Action

EBSA has made clear that cybersecurity relating to plan assets and PII should be a point of emphasis for ERISA plan sponsors and fiduciaries, as well as plan service providers. This goes beyond the requirements of HIPAA (applies only to group health plans) and applies to all service providers, whether business associates or not. Employers who sponsor ERISA-covered health and welfare benefit plans, should review the EBSA guidance, confirm current safeguards, and implement additional safeguards, as appropriate, primarily to protect data and to include holding service providers to high standards.

Actions to consider, include:

- identifying all current service providers with whom PII and health data may be shared.
- requesting current service providers to provide written representations of steps it takes to secure PII and health data from cyber threats.
- on a periodic basis (perhaps yearly), requesting current service providers to provide written updates on changes and other developments in its cybersecurity efforts.
- posing questions in the request for proposal ("RFP") pertaining to cybersecurity, including confirmation of:
  - a formal cybersecurity program, perhaps with certification (e.g., SOC 1 or SOC 2);
  - access control procedures;
  - cyber insurance, with policy limits;
  - training of relevant employees on cybersecurity awareness;
  - use of secured networks for exchanging confidential information, including by email; and
  - security assurance when using cloud service providers.
- educating plan members with respect to using sound online security practices, perhaps through furnishing members with the EBSA "Online Security Tips."