COMPLIANCE OVERVIEW

October 2024

Updated Cybersecurity Guidelines for ALL Employee Benefit Plans by the U.S. Department of Labor

The cybersecurity guidelines released by the Employee Benefits Security Administration (EBSA) in April 2021 are being confirmed by the EBSA to be applicable to all employee benefit programs, including group health plans.

To assist plan sponsors, fiduciaries, service providers, and participants in employee benefit plans in protecting plan data, private information, and plan assets, EBSA released cybersecurity guidelines in 2021. But in the intervening years, service providers for group health plans have informed fiduciaries and EBSA inspectors that this guideline is limited to retirement plans. In 2022, the ERISA Advisory Council of the Department of Labor suggested that EBSA make it clear that health benefit plans are covered by the guidelines.

The cybersecurity advice is applicable to all ERISA plans, including group health plans.

The guidance provides the below suggestions.

Best practices for hiring service providers include:

- Asking about the service provider's information security standards.
- Asking how a service provider validates its practices.
- Evaluating the service provider's track record in the industry.
- Asking whether the service provider has experienced past security breaches.
- Confirming the service provider has insurance policies that would cover losses caused by cybersecurity and identity theft breaches.

Federal Trade Commission (FTC) Cybersecurity Tips

Protect Your Files & Devices

Update your software:
This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files:
Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords:
Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices:
Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

***Use multi-factor authentication*:**
Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

This Compliance Overview is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Updated DOL Cybersecurity Guidance

-cont'd

Cybersecurity program best practices include:

- Having a formal, well-documented cybersecurity program.
- Conducting prudent annual risk assessments.
- Having a reliable annual third-party audit of security controls.
- Clearly defining and assigning information security roles and responsibilities.
- Having strong access control procedures.
- 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.
- Conducting periodic cybersecurity awareness training.
- Implementing and managing a secure system development life cycle (SDLC) program.
- Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypting sensitive data, stored and in transit.
- Implementing strong technical controls in accordance with best security practices.
- Appropriately responding to any past cybersecurity incidents.

Resources:

The new Compliance Assistance Release issued by the department's Employee Benefits Security Administration provides best practices in cybersecurity for plan sponsors, plan fiduciaries, recordkeepers and plan participants.

- 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 recordkeepers in mitigating risks.
- Online Security Tips: Offers plan participants who check their online retirement accounts with rules for reducing the risk of fraud and loss.

Federal Trade Commission (FTC) Cybersecurity Tips

-cont'd

Protect Your Wireless Network

Secure your router:

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption:

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders
solutions.

Make Smart Security your Business as Usual

Require strong passwords:

- A strong password is at least 12 characters that are a mix of numbers, symbols, and capital and lowercase letters.
- Never reuse passwords and don't share them on the phone, in texts, or by email.
- Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff :

Implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan:

Have a plan for saving data, running the business, and notifying customers if you experience a breach

This Compliance Overview is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.