



CYBERSECURITY GUIDANCE FOR EMPLOYEE HEALTH AND WELFARE PLANS

May 27, 2025

On Sept. 6, 2024, the U.S. Department of Labor issued Compliance Assistance Release No. 2024-01, which confirmed cybersecurity guidance that applies to all plans governed by the Employee Retirement Income Security Act (ERISA), including employee health and welfare plans.

Texas injury benefit plans, or non-subscription plans, are included in this guidance as they must comply with ERISA requirements that are applicable to welfare plans.

The guidance includes three tips, summarized below, which applies to plan sponsors, fiduciaries and participants, respectively.

1. **Hiring a Service Provider** – tips for plan sponsors and fiduciaries in selecting a security provider with strong cybersecurity practices as required by ERISA.
2. **Cybersecurity Best Practices** – tips for plan fiduciaries and service providers in implementing a strong cybersecurity program.
3. **Online Security Tips** – tips for plan participants in accessing retirement accounts and other employee benefit information online.

Hiring a Service Provider

Employers often rely on service providers to maintain employee health and welfare plan records and keep participant information confidential and secure. When selecting a service provider, employers and plan fiduciaries should focus on the following inquiries:

1. **Industry Standards:** ask about the service provider's security standards, practices and policies and audit results, and compare them with industry standards adopted by other financial/health institutions.
2. **Compliance Review:** ensure the service contract gives you the right to review audit results demonstrating compliance with security standards.
3. **Performance History:** evaluate the service provider's track record in the industry, including security incidents and litigation relating to the vendor's services.
4. **Prior Security Breaches:** ask the provider directly about prior security breaches and how they were handled.
5. **Insurance Policies:** ask whether the provider has insurance policies that would cover losses caused by cybersecurity breaches and the scope of coverage.
6. **Ongoing Compliance:** ensure the contract for services requires ongoing compliance with cybersecurity standards.

Cybersecurity Program Best Practices

These best practices apply to recordkeepers and other service providers who are responsible for online storage of plan-related data, and also to plan fiduciaries who make the decision on the service provider they should hire.

1. **Formal, Well Documented Cybersecurity Program:** A prudent program will address how to: identify risks to assets, information and systems; protect those assets; detect and respond to cybersecurity events; recovery from the event; disclose the event as appropriate; and restore normal operations.
2. **Annual Risk Assessments:** Employers should codify a risk assessment's scope, methodology and frequency.
3. **Annual Third-Party Audit of Security Controls:** The audit should provide an unbiased report of existing risks, vulnerabilities and weaknesses.
4. **Information Security Roles and Responsibilities:** An effective cybersecurity program must be managed by someone at the senior executive level who is qualified with knowledge of changing cybersecurity guidelines, risks and countermeasures.
5. **Strong Access Control Procedures:** Ensure procedures are in place requiring a user to prove they are who they say they are and have the appropriate access to systems and data.
6. **Assets or Data Stored in a Cloud or Managed by a Third-Party Service Provider:** See above section regarding Hiring a Service Provider to ensure participant information is kept confidential and secure.

7. **Periodic Cybersecurity Awareness Training:** Conduct training at least annually for all personnel and updated to reflect risks identified by the most recent risk assessment. Ensure plan participants are well-versed on the online security tips below.
8. **Secure System Development Life Cycle (SDLC) Program:** An SDLC program ensures security assurance activities like penetration testing, code review and architecture analysis are part of the system's development effort.
9. **Business Resiliency Program:** Implement a business resiliency program that will address business continuity, disaster recovery and incident response in light of a cybersecurity event or disaster.
10. **Encrypt Sensitive Data:** Ensure prudent standards for encryption are in place to protect the confidentiality and integrity of data at rest or in transit.
11. **Strong Technical Controls:** Maintain up to date hardware, software and firmware models; vendor-supported firewalls; and antivirus software. Also ensure routine patch management and data backup.
12. **Appropriately respond to any past cybersecurity incidents.** Provide appropriate notice; investigate the incident; honor any contractual or legal obligations with respect to the breach; and fix the problem to prevent its recurrence.

Online Security Tips

As an employer, ensure through necessary training that plan participants adhere to the following to reduce the risk of fraud and loss of personal data and assets:

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.

For additional guidance and information on ERISA compliance, please reach out to our ERISA compliance team.

Related Practices

Labor and Employment

Practice Area Contact

Sydney A. Shimkus