

US Department of Labor Compliance Assistance Release No. 2024-01:

Strengthening Cybersecurity in Employee Benefit Plans

Introduction

The digital age brings immense opportunities, but it also comes with significant challenges, especially in the realm of cybersecurity. One only has to look at a recent incident like the Change Healthcare data breach. Apart from the loss of trust, the prolonged outage of Change Healthcare's systems led parent company UnitedHealth Group to set up a Temporary Funding Assistance Program to aid struggling providers, paying around \$8.5 billion in loans under that program.¹ Since then, \$3.2 billion in loans have been repaid, and Change Healthcare has lost substantial business on top of it all. And that's only one snapshot of the potentially devastating risk security breaches can pose. As technology continues to advance, so do the techniques of hackers and cyber threats, opening new doors for security concerns. And when a business works with information as sensitive as private patient details and healthcare data, the need to meet those security concerns is more pressing than ever.

Recognizing the growing importance of protecting sensitive data, the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) has issued Compliance Assistance Release No. 2024-01. This release reaffirms the applicability of the previously issued cybersecurity guidance to all employee benefit plans, including health and welfare plans. With the continued intention of safeguarding the plan data, personal information, and plan assets, the release provides updated guidance to help plan sponsors, fiduciaries, service providers, and participants in employee benefit plans avoid the potentially catastrophic consequences of security breaches.²

Background and Purpose

The first Compliance Assistance Release from the EBSA provided guidance on conducting investigations, including the facilitation of voluntary compliance efforts, specifically those related to defined benefit pension plans' administration related to terminated participants.³ Key objectives were outlined for the Terminated Vested Participants Project, including common errors, the types of information requested, and how EBSA would work with plan fiduciaries to remedy any identified problems.

However, there was some initial ambiguity regarding whether the cybersecurity guidance issued in April 2021 applied solely to retirement plans or all employee benefit plans. Health and welfare providers informed EBSA investigators and fiduciaries that the guidelines applied only to retirement plans, showcasing a great deal of uncertainty around the initial guidance.² This prompted the ERISA Advisory Council to recommend a clarification, leading to the current release

Compliance Assistance Release No. 2024-01 outlines the optimal cybersecurity practices for plan sponsors, plan fiduciaries, recordkeepers, and plan participants of all plans under the Employee Retirement Income Security Act (ERISA).³ Plans that fall into this category include health plans, welfare plans, and all employee retirement benefit plans. The clarified cybersecurity guidelines now include:

- ✓ **Tips for hiring a service provider**
- ✓ **Cybersecurity program best practices**
- ✓ **General online security tips**

We'll be exploring the key components of those guidelines, as well as the best practices for adhering to the new release.

Key Components of the Updated Guidance

The updated guidance comprises several crucial elements aimed at bolstering cybersecurity measures across all employee benefit plans, most of which you're likely somewhat familiar with. As the risk of cyber-attacks continues to grow, following these guidelines, and fully understanding what they entail, is crucial.

1. Tips for Hiring a Service Provider

Choosing a service provider with strong cybersecurity practices is essential for the protection of highly sensitive plan data. Failing to protect vital data can lead to severe consequences, including financial penalties, data breaches, fraud, legal liabilities, and reputational damages.⁴ Hence, it's of utmost importance to select a provider that prioritizes cybersecurity and maintains robust protection measures, so health plans can ensure they meet regulatory compliance, prevent attacks, safeguard patient trust, and maintain operational continuity.

Here are our tips to get you started:

- ✓ **Evaluate Information Security Standards:** Assess the service provider's information security protocols to ensure they meet industry standards.
- ✓ **Review Audits and Track Record:** Investigate the provider's history, including any audits they have undergone, to gauge their reliability.
- ✓ **Insurance Coverage:** Verify that the provider has adequate insurance coverage to mitigate potential risks from cybersecurity breaches.
- ✓ **Contractual Provisions:** Ensure the contract includes robust cybersecurity provisions to safeguard plan data and participant information.

Service providers are the cornerstone of building strong cybersecurity practices. Through attentive measures and expert evaluation, healthcare organizations can mitigate the risk of cyber threats, avoid legal penalties, and ensure that patient trust is maintained.

2. Cybersecurity Program Best Practices

Implementing best practices is critical for managing cybersecurity risks effectively. Making sure your company has an official, well-documented cybersecurity program is a must, along with conducting annual risk assessments, ensuring trustworthy third-party audits, having defined security roles, conducting regular cybersecurity training, and more.⁵ Having a robust cybersecurity program in place can save you an immense amount of pain—and financial losses—in the long run, so it is vital to make sure the guidelines are followed to the best of your company's ability.

The guidance emphasizes the following:

- ✓ **Risk Management:** Develop and maintain a comprehensive risk management program to identify and mitigate cybersecurity threats.
- ✓ **Regular Monitoring:** Continuously monitor and evaluate cybersecurity measures to ensure their effectiveness and update them as needed.
- ✓ **Employee Training:** Conduct regular training sessions for employees to enhance their awareness and understanding of cybersecurity best practices.
- ✓ **Incident Response Plan:** Establish and maintain a detailed incident response plan to address any potential cybersecurity breaches swiftly and effectively.

3. General Online Security Tips

At its core, the release seeks to reduce the risk of fraud and prevent the loss to retirement accounts.⁶ This is best ensured by adhering to security best practices and hiring a trustworthy service provider, however, there are several other steps you can take to ensure the safety of digital accounts and information.

Some of these tips outlined by the release include:

- ✓ **Routine Account Monitoring:** Regularly check your retirement account balance and maintain online access to protect and manage your investments.
- ✓ **Use Strong Passwords:** Avoid writing your passwords down, sharing, reusing, or repeating passwords, and change them every 120 days.
- ✓ **Use Multi-Factor Authentication:** Set up a way for second credentials to verify your identity when logging in, such as entering a code sent to your personal phone or email.
- ✓ **Stay Cautious of Free Wi-Fi:** Use your cell phone or home network when accessing personal information to prevent security risks.

Conclusion

Compliance Assistance Release No. 2024-01 underscores the importance of robust cybersecurity measures in protecting the sensitive data associated with employee benefit plans. By adhering to the updated guidance, plan sponsors and fiduciaries can better safeguard their plans against cybersecurity threats. The inclusion of health and welfare plans in this guidance ensures

a comprehensive approach to cybersecurity across all types of employee benefit plans. With the digital landscape constantly evolving, organizations must stay vigilant and proactive in their cybersecurity efforts. The EBSA's updated guidance provides a valuable framework for achieving this goal.

About IPS

Dedicated to protecting sensitive data and keeping you and your business safe, Integrated Payor Solutions offers transformational, cloud-based solutions that power your payor or network business. Encompass+ is an ideal solution for your TPA, ASO, or network. A full-stack tech solution, Encompass+ removes the burden of having to invest in additional IT resources. Employers and providers can access through user-friendly portals, while detailed and customizable reporting means quick comprehension of that data. With Encompass+, you can grow your business while maintaining peace of mind that your data is safeguarded.

**Learn How IPS Can Help You
By Contacting Us Below!**

Sources

1. <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/>
2. <https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/compliance-assistance-release-2024-01>
3. <https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/retirement/missing-participants-guidance/compliance-assistance-release-2021-01>
4. <https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices>
5. <https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices>
6. <https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips>

**Connect with Us****Shawn Evans**

CEO, Integrated Payor Solutions

sevans@integratedpayorsolutions.com

415.465.2534