SEPTEMBER 19, 2024

SSG COMPLIANCE ADVISOR

What every HR leader should know about compliance.

DOL Confirms Cybersecurity Guidelines Apply to Health and Welfare Plans under ERISA

The Department of Labor's Employee Benefits Security Administration (EBSA) has confirmed in **Compliance Assistance Release No. 2024-01** that its cybersecurity guidance issued in April 2021 generally applies to all employee benefit plans, including health and welfare plans. In the prior guidance, the EBSA guidance focused on cybersecurity to mitigate risks to 401(k) and other retirement plans and to clarify that plan fiduciaries are responsible for managing cybersecurity issues. With the new guidance, the EBSA is making it clear that plan fiduciaries must monitor cybersecurity risks for all types of ERISA plans, not just retirement plans.

Background

EBSA cybersecurity guidelines require plan fiduciaries to take appropriate precautions to mitigate the risk of harm due to cybersecurity incidents. The DOL's cybersecurity guidance was released in three parts addressing all plans with a few minor updates to the 2021 guidelines:

1. **Tips for Hiring a Service Provider with Strong Cybersecurity Practices**
2. **Cybersecurity Program Best Practices** for recordkeepers and other service providers
3. **Online Security Tips** for plan participants and beneficiaries who check and manage their accounts online

While this guidance is published as compliance "tips" and suggested "best practices," rather than mandates for plan fiduciaries, in practice, the DOL in plan audits has questioned sponsors about implementation of these best practices as minimum expectations for plan fiduciaries to comply with their obligation to manage cybersecurity risks.

For group health plans, of course, cybersecurity requirements already apply under the HIPAA Privacy and Security Rules. Sponsors of self-insured plans who have delayed adopting HIPAA Privacy and Security Policies should consider doing so now in light of this focus by the DOL on cybersecurity issues. Final Rules recently issued under HIPAA earlier this year also require group health plans to update their HIPAA privacy policies and procedures and provide associated workforce training by December 22, 2024. Accordingly, now is a good time to ensure HIPAA compliance as well.

Tips for Hiring a Service Provider

The DOL provides suggested questions to ask potential service providers to evaluate that service provider's cybersecurity practices. This includes asking the service provider about their information security standards, audit policies and results, how it validates its practices, what levels of security standards it has met and implemented, and past security breaches. The 2024 updates require fiduciaries to ask about insurance coverage for cybersecurity incidents and breaches. The responses should be considered against other potential service providers, industry standards, and the service providers track record.

The DOL guidance also suggests careful attention to the service contract which should, among other things:

- Require the service provider to obtain third-party audits on an annual basis.
- Identify how quickly a service provider must inform plan fiduciaries of breaches.
- Specify the service provider's obligation to meet applicable federal, state, and local laws regarding privacy, confidentiality, or security of participants' personal information.

Cybersecurity Program Best Practices

The DOL has identified a 12-point best practice system for use by recordkeepers for plan-related IT systems and for use by plan fiduciaries in making prudent decisions regarding cybersecurity measures.

1. **Have a formal, well-documented cybersecurity program.** This includes a system to identify risks, protect assets, data and systems, detecting and responding to cybersecurity events, recovering from the event, disclosing (as appropriate), and restoring normal operations and services. This program should be approved by senior leadership, reviewed internally at least annually, and be reviewed by an independent third-party auditor to assess compliance and threats.
2. **Create a prudent, annual risk assessment program.** Establish a manageable, effective risk assessment schedule to identify and assess cybersecurity risks and to describe how the program will mitigate identified risks. This program should be updated to account for changes to information systems, service providers, or other changes to business operations.
3. **Engage a third-party annual audit of the security controls.** In addition to the internal measures adopted, an independent third-party auditor should assess the security controls on an annual basis. If the auditor's report identifies any weaknesses, the plan fiduciary should also document the correction of any identified weaknesses.
4. **Clearly define and assign information security roles and responsibilities.** The DOL specifically recommends that a cybersecurity program be managed at the senior executive level and then executed by qualified personnel. The Chief Information Security Officer (CISO) would generally be an appropriate individual to establish and maintain the program.
5. **Ensure strong access control procedures.** Establish an authentication and authorization procedure to guarantee that users are who they say they are and that only approved users can access IT systems and data. The 2024 update recommends use of multi-factor authentication (MFA) and a notice to individuals when unauthorized access has occurred.
6. **Assess third-party service provider use of cloud computing.** This assessment should be part of the decision to engage with a service provider. This would include requiring a risk assessment of the third-party service provider, periodically assessing the service provider, and ensuring that the guidelines of any safety program are satisfied.
7. **Conduct annual cybersecurity awareness training.** A strong procedure should address risk from each level, including the employee level. Accordingly, the DOL suggests conducting an annual cybersecurity awareness program to educate everyone to recognize attacks, help prevent incidents, and guard against identify theft.
8. **Implement a secure system development life cycle (SDLC) program.** A secure SDLC program ensures that security assurance activities, such as code review, are an integral part of the system development process.
9. **Implement a business resiliency program to address business continuity, disaster recovery, and incident response.** Business resilience is the ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. The DOL proposes creating a business continuity plan, disaster recovery plan, and an incident response plan.
10. **Encrypt sensitive data.** Implement current, prudent standards for encrypting data that is stored and data that is transmitted.
11. **Implement strong technical controls to implement best security practices.** Implement controls that keep hardware, software, and firmware up to date, conduct routine data backup, and ensure routine patch management.
12. **Be responsive to cybersecurity incidents or breaches.** Ensure appropriate action is taken to protect the plan and plan participants in the event of a cybersecurity incident or breach. Actions may include informing law enforcement, notifying insurers, investigating the incident, and fixing the problem or weakness that caused the breach.

Online Security Tips

The final component of the DOL guidance focuses on actions that plan participants and beneficiaries can take to mitigate potential cybersecurity risks. These tips include:

- Regular monitoring of accounts
- Using strong passwords with multi-factor authentication
- Updating personal contact information
- Signing up for account activity notices.

The DOL also provides individuals with some general best practice considerations when accessing accounts or having an online presence generally, such as being aware of phishing attacks, using antivirus software, and updating apps and software regularly. The 2024 guidance modified the recommended frequency for password changes by participants to annually rather than every 120 days, noting that participants favor longer more complicated passwords over frequent updates.

Employer Action Items

- Cybersecurity has been an increasing concern as processes and platforms have increasingly moved to remote or electronic providers. Given this landscape of electronic services and the DOL's recent guidance, plan fiduciaries should:
- Conduct a cybersecurity self-audit of internal practices and safeguards (considering HIPAA compliance as well for group health plans subject to both the ERISA fiduciary guidelines for cybersecurity protections and HIPAA Privacy and Security Rules).
- Identify gaps in current plan sponsor and fiduciary practices compared to the DOL guidance and take necessary steps to ensure plan fiduciaries can fulfill obligations to protect the plan from cybersecurity risks.
- Review the Hiring Tips and conduct an audit of current vendors and recordkeepers, making sure that any future RFPs follow the outlined practices from the EBSA.
- Provide the Online Security Tips guidance to employees and plan participants.
- Document the steps taken to comply as part of the fiduciary governance process and oversight of health and welfare plans in addition to retirement plans.