Enhanced Cybersecurity Guidance for ERISA Plans

By Kevin Brady

In April 2021, the U.S. Department of Labor (DOL) released guidance on best practices for cybersecurity. Initially aimed at retirement plans, the guidance broadly applies to all plans covered by the Employee Retirement Income Security Act (ERISA).

Recently, the DOL updated its guidance, explicitly confirming its applicability to health and welfare plans. Even for sponsors of plans not governed by ERISA—such as government and most church plans—the insights provided in the guidance are invaluable and worth reviewing.

Why focus on service providers?
The guidance primarily addresses the responsibilities of service providers to ERISA plans because at the end of the day, that's where the data resides.

While employers often handle sensitive employee information, they usually lack direct access to the comprehensive data service providers possess. For example, insurers or third-party administrators (TPAs) maintain extensive health claims data that employers typically do not access due to Health Insurance Portability and Accountability Act (HIPAA) limitations.

Key components of cybersecurity best practices
The updated guidance retains the original framework, with minor refinements, for creating a robust cybersecurity program. The DOL outlines the following critical elements for service providers:

1. **Develop a documented cybersecurity program.** Clearly define risks, protection strategies and response measures to address cybersecurity events effectively.
2. **Enforce robust access control procedures.** Ensure that only authorized individuals access sensitive data.
3. **Implement strong technical controls.** Effective defenses deter potential attackers and reduce system vulnerabilities.
4. **Deliver regular cybersecurity training.** Employees often constitute the weakest link. Training reduces the likelihood of phishing attacks and other human errors.

5. **Define clear roles and responsibilities for information security.** Avoid the pitfall of making cybersecurity "everyone's job" by assigning specific accountability.
6. **Evaluate third-party and cloud provider security.** If data is stored externally, the service provider's security measures must meet stringent standards.
7. **Encrypt sensitive data at rest and in transit.** Encryption safeguards data from unauthorized access.
8. **Perform annual risk assessments.** Regular evaluations keep the program relevant to emerging threats.
9. **Secure independent audits of security controls annually.** External audits offer unbiased insights into strengths and vulnerabilities.
10. **Adopt a secure system development life cycle.** Internal application development processes must prioritize security.
11. **Create a business resiliency program.** Plan for continuity, disaster recovery and incident response to mitigate disruptions.
12. **Respond effectively to past cybersecurity incidents.** Thorough investigations and corrective actions help prevent recurrence. Notifying insurers and law enforcement, when appropriate, is also essential.

The DOL's recommendations are not one-size-fits-all. Each service provider's practices should be modified to align with the sensitivity and scope of the data they manage. For instance, a provider handling comprehensive health claims data should implement more stringent measures than one managing less sensitive information. Employers are responsible for evaluating whether a service provider's cybersecurity approach is adequate for the data under their purview.

Practical applications for plan sponsors
Health and welfare plan sponsors will find that many vendors already emphasize cybersecurity, partly due to the 2021 HIPAA-driven legislation and a number of cybersecurity events that have been highly publicized in recent years. However, the DOL's guidance serves as a valuable checklist for sponsors to evaluate their service providers through a fiduciary lens.

The package includes a document titled "Tips for Hiring a Service Provider with Strong Cybersecurity Practices." While HIPAA offers a broad framework for data security, the DOL's recommendations provide more detailed and actionable insights. Sponsors should use this resource to ask pertinent questions, obtain meaningful responses, and document their decisions to fulfill fiduciary obligations.

In addition to reviewing service providers, sponsors should assess their internal cybersecurity measures, especially if they retain sensitive plan-related data. ERISA's "prudence" requirement hinges on adopting a sound process—a hallmark of effective fiduciary responsibility. This involves:

- Asking relevant questions about cybersecurity measures.
- Evaluating answers based on established standards.

- Making informed decisions and documenting them thoroughly.

The bigger picture
The updated guidance underscores the significance of robust cybersecurity for all ERISA-covered plans, including health and welfare plans. It highlights the critical role of service providers in safeguarding sensitive data and emphasizes the need for sponsors to evaluate these practices rigorously. While many providers already adhere to high standards, the DOL's checklist offers an opportunity for continuous improvement.

Even if a plan is not subject to ERISA, following these best practices can help mitigate risks and enhance data security. Taking proactive steps to address cybersecurity not only protects employees' sensitive information but also bolsters an organization's compliance posture and reputation. In today's complex digital environment, prioritizing these measures is more crucial than ever.

About the author:
Kevin Brady is global insurance brokerage Hub International's Chief Compliance Officer. He provides compliance and consulting services regarding group health plans and other employee benefits. He consults with employers to design, implement and ensure the compliance of employee benefits plans with the Affordable Care Act, ERISA, Internal Revenue Code, HIPAA, COBRA, FMLA, ADA and related matters.