COMPLIANCE ALERT

Revisiting the DOL's Cybersecurity Guidance

April 3, 2023

Quick Facts

- In July 2021, the Department of Labor (DOL) released cyber security **"best practice" guidance** for Employee Retirement Income Security Act (ERISA) plan sponsors.
- It appears that the DOL is establishing best practices and expectations for plan sponsors with respect to their service providers and what to expect in the event of an audit.
- Employers as plan sponsors should take reasonable steps to implement cybersecurity practices within their organizations.

Background

In July 2021, the DOL released cyber security **"best practice" guidance** for ERISA plan sponsors. The guidance was presented as "best practices" and not official requirements but appeared to establish expectations for ERISA plan sponsors. Recent DOL cybersecurity-related questions appear intended for employer plan sponsors, establishing best practices and expectations for employers and their service providers and what they might expect in the event of an audit. Below is a summary of common questions from DOL audits, possible implications, and next steps for employer best practices.

DOL Audit Questionnaires

Questions listed below have appeared on DOL recent employer audits.

1. Documents sufficient to describe password protocols for participant Plan accounts, including the number and type of characters, the frequency with which it can be changed or need to be changed, and the complexity required;
2. Documents sufficient to describe the encryption protocols for Plan data including firewalls, antivirus software (including subscriptions), and data backup;
3. Brief description of how Plan Sponsor access Plan's data for entering information;
4. Names and titles of persons who have access to Plan data and extent of their access, i.e., census, payroll, participant information, etc.;
5. Documents pertaining to any cybersecurity training for the Plan Sponsor's employees and its fiduciaries;
6. A brief narrative describing any past cybersecurity breaches involving the Plan and its participants including the extent of the breach and changes implemented to prevent future cybersecurity violations;
7. Cybersecurity Liability Policy and related documents, if applicable;
8. Documents provided to the Plan Sponsor by service providers in regard to cybersecurity protocols for maintaining Plan data;

9. Copies of any documents distributed to Plan participants encouraging cybersecurity awareness; and
10. Documents pertaining to any changes or updates to the basic Plan Documents or Summary Plan Documents relating to cybersecurity protections, assessments, and internal controls.

What Does This Mean?

The set of questions above tells us some things but raises other questions. It suggests that the DOL does, in fact, expect plan sponsors to take cybersecurity seriously. Many of the issues it raised in the 2021 guidance are now showing up on actual audits, but not all these audit questions appear to stem directly from the guidance. For example, the 2021 guidance said nothing about procuring cybersecurity insurance, although that could be considered a logical step for anybody taking the guidance seriously. The 2021 guidance was primarily focused on how plan sponsors should select/audit their service providers and on the types of safeguards those service providers should have in place. The DOL audit questions appear directed at the employers themselves. This begs the question: should employers answer these questions on behalf of their plan service providers, or should they be implementing these requirements themselves?

An additional question raised by these audit questions raise is if the DOL intends to penalize plans if they conclude the plan has not done enough to protect against cybersecurity threats. Further, can they even do so? On one hand, given that the 2021 guidance was issued as best practices and not regulatory requirements, it seems unlikely the DOL could penalize a plan for not following specific steps in those guidelines. On the other hand, if the DOL believes the plan has not taken cybersecurity seriously overall, it's possible the DOL will require specific corrective action under ERISA's fiduciary requirements or some similar general obligation to protect the plan and its participants.

Should employers implement all of the DOL guidelines exactly as written to protect themselves in the event of an audit? Not necessarily, but employers should pay attention to cybersecurity issues as they apply to their benefit plans and correct any obvious gaps in their existing practices. Many of the DOL best practices involve actions the employer may already be taking to protect against cybersecurity threats to its overall business.

The same is true with privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA). Many of the things an employer must do to properly implement HIPAA's privacy and security requirements for the group health plan are applicable to other benefit plans not subject to HIPAA. HIPAA compliance might go a long way toward satisfying the DOL's concerns in an audit if they were expanded slightly. The goal should be to provide enough positive responses if the employer is subject to a DOL audit, demonstrating that the employer is taking the issue of cybersecurity seriously.

Practical Implications and Next Steps

There are several steps employers can implement to be ready for a possible DOL audit.

As plan sponsors, employers should take reasonable steps to implement cybersecurity practices within their organizations and protect any plan data that is stored/accessed internally. Their vendors/service providers should also be implementing these requirements for the data they handle.

Employers should comprehensively review their existing information technology (IT) security practices in light of the 2021 guidance and DOL audit questions. Plan sponsors should document how those existing practices are applicable to their benefit plans in order to ensure that they are prepared to respond to these inquiries on behalf of their service providers and their own organization.

While HIPAA compliance efforts may not address all ERISA plans sponsored by an employer, they will provide a meaningful framework to apply to any plans that fall outside HIPAA's scope. If employers have not yet addressed HIPAA's privacy and security requirements, including written policies and procedures and conducting a HIPAA security risk analysis, they should make this a priority.

The third section of the 2021 guidance focused on cybersecurity practices for participants/individuals. While not explicit, there may be an expectation that plan sponsors communicate these best practices to individuals via some sort of notice. This section of the guidance was written as a two-page summary directed at plan participants themselves. It could work as a model notice to provide to employees as part of the annual notices packet, or in a benefits enrollment booklet, or as part of an organization's existing security awareness training initiatives. Employers should look at the summary document and compare it to what it may already be communicating to its employees/plan participants through things like Acceptable Use Policies.

Summary

It appears that the DOL has used the 2021 guidance to communicate its expectations for how employers and their vendors should be safeguarding their plan data. Ensuring compliance with these expectations should not be an entirely new undertaking. After reviewing existing IT security efforts and HIPAA security compliance efforts, employers will likely find that many of the 2021 guidance "best practices" are already being addressed to some extent. Employers who have not yet undertaken compliance efforts with respect to HIPAA privacy and security should take the time to address those requirements now.

EPIC Employee Benefits Compliance Services

For further information on this or any other topic, please contact your EPIC benefits consulting team.