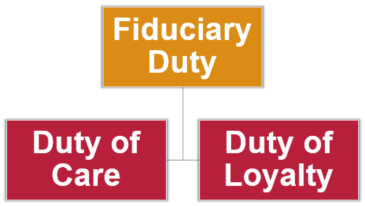
JULY 21, 2021

Fiduciary Duty IS Coming to Privacy – Through Your Benefit Plans!

by R. Sterling Perkinson , Jon Neiditz , Anthony D. Glosson



While all businesses have been grappling with cybersecurity challenges for years, cybersecurity has recently come into focus for retirement plans, health and welfare plans and other ERISA plans due to a new Department of Labor ("DOL") cybersecurity initiative. As discussed in our previous ERISA blog post, the DOL issued several pieces of data privacy and cybersecurity guidance in April.

The DOL has quickly followed up on this guidance by incorporating privacy and cybersecurity requests into its audits of employee benefit plans. The DOL's cybersecurity request list covers employers' internal data privacy and security policies, as well as those of third party service providers who have access to employee data. The requests may also cover secondary uses of employee data, such as for marketing or cross-selling purposes or other monetization. We have outlined considerations for plan fiduciaries, including employers and investment or administrative committees, to document that they have followed a prudent process to protect the plan from losses from cybersecurity events and to protect the personal data of participants and beneficiaries.

Review Cybersecurity Policies and Procedures When Engaging Service Providers

Employers and other plan fiduciaries responsible for hiring plan service providers should assess cybersecurity policies and procedures of service providers before entering into contracts for services involving the plan. Many plan service providers handle personal data, including recordkeepers or third party administrators, actuaries and auditors. Fiduciaries should enlist their company's internal experts or outside consultants from the beginning of the procurement process to help assess cybersecurity policies and procedures.

- Request cybersecurity policies and procedures as part of any request for proposal (RFP) for a service provider that may be handling participant data so that they may be evaluated before engaging the service provider.
- When a service provider has had a recent acquisition, review documentation to confirm that cybersecurity policies and procedures have been fully integrated and are consistent throughout the organization.
- Incorporate cybersecurity policies and procedures that protect the personal data of participants and beneficiaries into service provider agreements, including:

- o Representations and warranties regarding compliance with policies and procedures, including third party audits
- o Prohibitions on sharing participant or beneficiary data or unauthorized use of data such as for marketing or cross-selling purposes
- o Requirements for appropriate levels of insurance coverage for cybersecurity incidents
- o Requirements for prompt initial notification of cybersecurity incidents within a specific time period (e.g. 48 hours)
- o Requirements to provide audit reports or access to other information that will help to assess compliance with data privacy and security policies and procedures

Review and Monitor Cybersecurity Compliance on an Ongoing Basis

The fiduciary duties of ERISA require that employers and other plan fiduciaries continue to monitor the performance of plan service providers after they are engaged. This review should be reflected in the formal documents of the fiduciaries, such as in meeting minutes of an investment or administrative committee. This review may include the following:

- Request cybersecurity policies and procedures for existing plan service providers to evaluate data security and privacy protections with the assistance of internal experts or outside consultants.
- Request and review third party audit reports or assessments of service providers regarding compliance with cybersecurity policies and procedures.
- Review existing service provider contracts to assess the cybersecurity protections and whether amendments are necessary to better protect employee data.
- Periodically invite key service providers, like recordkeepers, to present to plan fiduciaries on their cybersecurity policies and procedures. Internal experts or outside consultants should also be invited to meetings where cybersecurity is on the agenda so they can help assess the policies and procedures and ask questions to service provider representatives directly.

Review of Internal Systems

The DOL's cybersecurity initiative may cover any company systems that are involved in employee benefit plan administration (for example, if pension calculations are performed internally). As a result, it is important to document that appropriate privacy and security policies and procedures are in place. This documentation may include:

- Assessments of security risks
- Processes for business continuity, disaster recovery and incident response
- Documentation of security reviews and assessments of assets stored in a cloud or managed by service providers
- Cybersecurity incidents reports
- Cybersecurity awareness trainings

Document Review Process

Plan fiduciaries, including employers and investment or administrative committees, should be able to

show that they have taken appropriate steps to protect employee data. The fiduciary standards of ERISA are process-based, meaning that fiduciaries must document that they have followed a prudent process, regardless of outcome. As a result, maintaining records of compliance with data privacy and security policies and procedures in the official records of a fiduciary, such as in committee meeting minutes or formal reports, is critical to showing that fiduciaries have satisfied their fiduciary duties with respect to protecting the data of plan participants and beneficiaries.

One the biggest controversies in the privacy regulatory world is whether to give organizations fiduciary responsibilities over consumer data. Given the regulatory framework fundamental to plans, plans may in fact be the national leaders in this way of thinking about privacy.