Subscribe To Data Privacy Law

Email Address *

SUBSCRIBE!

Search Posts

Categories

- Webinars & Podcasts
- Jaffe Updates
- News
- Electronic Payments Law +
- Michigan Green Law +
- Data Privacy Law +
- Immigration Law +

Download PDF

JULY 24, 2018 | DEBORAH BAUGHMAN

Data Security for Retirement Plans

If you are an employer, there is a good chance you sponsor a qualified retirement plan, such as a 401(k) plan, and offer your employees coverage under a group health plan. These employee benefit plans maintain a lot of detailed personal information about participants and their families, including, names, dates of birth, Social Security numbers, bank information, compensation, medical claims data, email, and physical addresses, and account balances. This personally identifiable information ("PII") is shared with and accessed by different users and service providers to administer the plans. In this age of ever-increasing cybersecurity threats, how safe is PII collected, used, and disclosed from a data breach?

These federal laws contain privacy provisions applicable to individually identifiable health information maintained, used, or disclosed by group health plans:

- Health Insurance Portability and Accountability Act;
- Genetic Information Nondiscrimination Act;
- Gramm-Leach-Bliley Act;
- Americans with Disabilities Act;
- Federal Trade Commission Act;
- Federal Substance Abuse Rules;
- Federal Computer Fraud and Abuse Act;
- Federal Constitutional Rights of Privacy for Medical Records; and
- Federal Identity Theft Prevention Program

Although many federal and state laws deal with privacy and security, there is no comprehensive federal legislation, including ERISA, which protects data maintained for use by your retirement plan or third party administrator. You may need to develop your own strategy to protect and monitor the PII of participants in your retirement plan.

In 2011 and again in 2016, the ERISA Advisory Council (consisting of 15 members appointed by the Secretary of Labor to advise the Secretary and make recommendations), examined cybersecurity considerations as they relate to pension and welfare benefit plans. In 2011, the Council urged the Department of Labor to provide guidance concerning protecting PII as a fiduciary responsibility and the extent to which participant and beneficiary PII should be protected while administrating the plans. To date, no guidance or legislation dealing with privacy and security of PII maintained by retirement plans has been proposed.

The 2016 Council focused on cyber risk management strategies that can be scaled (no one-size-fits-all) based on the sponsor, its resources, plan size and complexity. The Council prepared a cybersecurity educational resource titled "Employee Benefit Plans: Considerations for Managing Cybersecurity Risks".

The Council focused on these elements to develop a cybersecurity risk management strategy.

- Understand Participant Data
    - What data should be protected?
    - How is the data classified? (PII vs. protected health information ("PHI"), with different standards of care)
    - Where is the data stored? (multiple parties/locations)
    - Who has access to the data?
    - How is data accessed?
    - Is access controlled; are there procedures in place to manage access?
    - What data is needed?

- What data must be retained?
- What are the threats?

- Cybersecurity Frameworks – below follows the framework developed by the National Institute of Standards and Technology
  - Identify risks (including employees who may be careless or poorly trained)
  - Develop a program to protect data that could be at risk (create a culture of awareness, update software and security)
  - State how breaches will be detected
  - Develop a plan to respond once a breach occurs
  - Detail plan of recovery

- Protocols and Policies
  - Implementation and monitoring (who designs, documents, implements, and maintains the (dynamic) strategy)
  - Testing, updating, enhancing cybersecurity procedures
  - Regular reports to fiduciaries
  - Regular cyber risk awareness training
  - Background checks on new personnel
  - Restrict access to an as-needed basis
  - Strategy to remove unnecessary data
  - Evaluate service provider security programs and access to data

- Striking the Right Balance
  - Determine the balance of preventive measures relative to the probability of the threat, loss exposure, and cost of protective action

The challenges will continually evolve. Consider hiring a professional to help you protect the PII maintained by the retirement plan if you do not have the expertise in-house. You may also want to consider whether cybersecurity insurance makes sense for your company. Check existing insurance policies to determine what is included or excluded should there be a cyber breach – and how it compares to the risks identified. Do not forget to review the cyber protections in place at your service providers. Everyone who comes in contact with PII or PHI must be conscientious. Be aware of these sensitive issues.