Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Considering Best Data Practices For ERISA Fiduciaries

*Law360, New York (May 5, 2015, 1:32 PM ET) --*

Michelle Capezza

Employee benefit plan fiduciaries are charged with meeting a prudence standard when discharging their duties solely in the interest of plan participants and beneficiaries. With increasing regulation of benefit plans, these duties and associated responsibilities are mounting. With advancements in technology, online enrollment and access to account information, as well as benefit plan transaction processing, participant identifiable information and data have become increasingly more vulnerable to attack as it travels through employer and third-party systems.

Earlier this year, the attack on Anthem Inc.'s information technology system, which compromised the personal information of individuals under numerous health plans (including personally identifiable information, bank account and income data, and Social Security numbers), raised questions of privacy and security under the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act, and there have been other similar attacks.

These cases remind us that in today's world, plan participant information, whether it be protected health information, personally identifiable information or retirement savings account information, is vulnerable to theft. Employee Retirement Income Security Act plan fiduciaries must not only act prudently in responding to a breach of their plan participants' PHI, but should also consider developing prudent policies and procedures with respect to the handling and transmission of all PII and participant data in the regular course.

In 2011, the Advisory Council on Employee Welfare and Pension Benefit Plans studied the importance of addressing privacy and security issues with respect to employee benefit plan administration. The council examined issues and concerns about potential breaches of the technological systems used in the employee benefit industry, the misuse of benefit data and PII and the impact on all parties, including plan sponsors, service providers, participants and beneficiaries. The council recognized several potential causes of breaches relating to benefit plan information, including hacking into retirement plan financial data, and recommended that the U.S. Department of Labor provide guidance on the obligation of plan fiduciaries to secure PII and develop educational materials. To date, the the Department of Labor has issued no such guidance.

**What are the Concerns Identified by the Council?**

Some of the concerns and areas of vulnerability addressed by the council include: (1) theft of personal identities and other PII, (2) theft of money from bank accounts, investment funds and retirement accounts, (3) unsecured/unencrypted data, (4) outdated and low-security passwords, (5) hacking into plan administration, service provider and broker systems, (6) email hoaxes and (7) stolen laptops or data hacked from public computers where participants logged into accounts.

The council concluded that addressing these issues requires consideration of all stakeholders who share, access, store, maintain and use PII, including, but not limited to, participants, plan sponsors, plan administrators, third-party administrators, record-keepers, investment advisors, other service providers, trustees and other fiduciaries. Issues to be considered, as set forth by the council, include privacy policies which address who may have access to PII, procedures for disseminating information concerning PII security breaches and remediation when breaches result in financial harm to plan participants and/or beneficiaries.

Developing a roadmap to remediation of financial harm may be easier said than done, however, especially given the difficulty in measuring a financial injury that may or may not occur in the future as a result of PII being stolen from an employee benefits plan or an individual participant's account. Social Security numbers, for example, may not be used to steal an individual's benefits for many years after a data breach and any subsequent lawsuit. Even if theft of Social Security numbers is directly linked to a quantifiable financial loss, plans that outsource record-keeping responsibilities to third-party administrators place fiduciaries in uncharted waters if the plan is governed by state laws that prohibit the disclosure of Social Security numbers to third parties.

Indeed, drafting an appropriate PII privacy and protection policy is quickly complicated by the sheer fact that this area of concern is evolving and questions regarding ERISA preemption and conflicts with state and federal data privacy laws are not yet definitively addressed. With federal cybersecurity legislation on the horizon, state laws on data breach notification already on the books, scrutiny over financial institutions and their compliance with laws designed to protect PII, and the increasing importance on HIPAA and HITECH compliance in the wake of health plan data breaches, merely understanding the ambit of ERISA fiduciary obligations to protect against employee benefit plan participant data breaches presents a challenge.

**What Standard of Care Applies to Fiduciaries?**

Under ERISA, a fiduciary shall discharge his duties with respect to a plan solely in the interest of the participants and beneficiaries, for the exclusive purpose of providing them benefits and defraying reasonable expenses of administering the plan. A fiduciary must do so in accordance with the documents and instruments governing the plan and with the care, skill, prudence and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims. A fiduciary may breach these duties with his or her action or inaction.

For instance, a 401(k) plan fiduciary that does not prudently select and monitor the investments offered under a plan or the managers of plan assets could potentially be held personally liable for breaching his or her fiduciary duties if participants and beneficiaries are financially harmed by imprudent investments. Department of Labor guidelines provide, however, that so long as the plan fiduciaries follow prudent

procedures to select and monitor plan investments, the fiduciaries are not necessarily liable for the performance of such investments. Although there is guidance plan fiduciaries can follow to properly select and monitor plan investments and service providers, as pointed out in the council's 2011 report, there is no clear guidance on the level of responsibility fiduciaries have to protect PII nor the appropriate standard of due diligence that should be used to evaluate service provider controls over the security and privacy of PII.

**What Should Benefit Plan Fiduciaries Do in the Absence of Clear Rules Regarding Protection of PII?**

As with other plan administration responsibilities, it is important for plan fiduciaries to establish and follow prudent practices and procedures for handling and securing PII, including when the handling and securing of such data is delegated to third parties (i.e., a "PII privacy and protection policy"). It is critical for plan fiduciaries to develop appropriate protocols in these policies, evaluate the type of data and information that will be transmitted and where it will be transmitted. Keep in mind that security measures should be tailored to a particular organization depending on their role in the benefits administration and the interface between them and the other stakeholders in the plan.

When it comes to prudent selection and monitoring of plan service providers that will handle PII, due diligence of the third-party service provider's systems, data storage and encryption security are all critical. It is equally important to prudently delegate responsibilities to company personnel that will handle PII.

Plan sponsors and other fiduciaries are well-advised to consider the following when preparing individualized PII privacy and protection policies and to require third-party service providers to demonstrate compliance.

***Data***

- Keep only data that is needed and use effective processes to discard unnecessary data, including backup paper and electronic copies.

- Know where PII is located in all of the organization's systems, and understand the security levels of any cloud computing and remote data storage processes that are involved in plan administration, including how data is stored or protected.

- When protected health information is at issue, follow HIPAA/HITECH guidelines.

***Systems***

- Keep computer systems updated, including prompt installation of software patches and stay current on electronic threats and effective responses.

- Follow National Institute of Security and Technology guidelines on computer configuration use.

- Use full disk encryption on laptops and external data storage devices that might include PII or information on how to access it.

- Maintain complete login for the network, firewalls, routers and key software applications, and limit or define usage of portable devices.

***Service Provider Management***

- Delegate duties responsibly and prudently monitor third parties and employees with access to plan data.

- Address privacy and security factors when vetting and selecting providers.

- Assess the service providers' certifications in privacy and security and request information regarding past data breaches.

- Request information regarding service providers' processes and systems for addressing cybersecurity threats and protection of PII.

- Make sure third-party provider subcontractors are held to same standards as the service provider.

- Develop a record of diligence efforts undertaken to document the level of security of third-party service providers and that their systems and methods for handling, storing and retrieving data are compliant with state of the art security measures.

- Engage the expertise of company IT professionals and your legal counsel to review service agreements and provisions regarding data security and confidentiality, and develop parameters for indemnification in service agreements.

- Review a copy of each third-party service provider's Statement of Auditing Standards No. 70 report regarding its system controls.

***Special Concerns for Employees***

- Educate employees about the importance of safeguarding their data at all times and warn against email and phishing scams.

- Encourage use of passwords with a high level of security and that they are updated regularly.

- Advise participants and beneficiaries to monitor their accounts.

- Focus on security measures in place for plan distributions, loans and withdrawals. Ensure added security for participants at time of distribution.

- Prepare communications that remind participants and beneficiaries to safeguard their own benefit information, account balances, health information, passwords and PINs, and advise against placing too much personal information on social networking sites and reviewing sensitive data on public computers or kiosks.

***People and Training***

- Perform background checks on all individuals with access to PII.

- Ensure all personnel who have access to PII are trained in properly safeguarding it. Include training in areas such as data retention/destruction, social networking, social engineering and litigation holds.

- Designate an individual to be in charge of privacy and security of PII, educate all stakeholders regarding appropriate focus according to their roles, and implement and test contingency plans for use in event of data breach.

**General Tips**

- Keep records of any breach investigations and steps taken to remedy the breach.

- Review fiduciary liability insurance and consider potential interplay between cybersecurity insurance.

- Perform periodic risk assessments (Generally Accepted Privacy Principles), maintain good controls and be careful about who can override them.

- Consider updating plan documents to incorporate the PII protection and privacy policy.

- Use a process to confirm compliance with the policy and make sure the policy is clear and communicated to all appropriate parties.

In this ever changing landscape, these considerations are not definitive or finite. Development of best practices, including a PII privacy and protection policy, will require thought and insight depending on the facts and circumstances. In the absence of formal guidance, it is imperative for plan sponsors and fiduciaries to address these issues and develop best practices and procedures that are suitable to prudently administer their plans in the information/innovation age.

—By Michelle Capezza and August E. Huelle, Epstein Becker & Green PC

*Michelle Capezza is a member of the firm and August Huelle is an associate in Epstein Becker & Green's New York office.*