Client Advisory

pillsbury

Privacy, Data Security and Information Use

Health Law

Global Sourcing

Executive Compensation & Benefits

Finance

September 6, 2016

Cybersecurity and the Role of ERISA Fiduciaries

By Susan P. Serota, Christine L. Richardson, Allen Briskin and Jessica Lutrin

The Employee Retirement Income Security Act of 1974, as amended (ERISA), protects plan participant benefits and account balances by imposing high standards of care on the plan's fiduciaries. Fiduciaries who do not follow these standards—most notably, the protection of participant personal and plan information—may be personally liable to restore losses to the plan. Recent technological advancements, especially in the area of cybersecurity, however, have only now become the focus of most ERISA fiduciaries. Due to the increasing frequency and sophistication of cyber-related threats to employee benefit plans, their trustees and third-party plan administrators and the potential financial repercussions, compliance with ERISA fiduciary standards will require implementation of a prudent cyber risk management strategy.

This advisory is the third in a series of advisories dedicated to understanding cybersecurity issues in the context of ERISA benefit programs.[1]

ERISA Fiduciary Duties

ERISA sets forth the duties and standards of conduct for those individuals and entities that exercise discretion or control over the management and administration of employee benefit plans and their assets, that is, fiduciaries. Fiduciaries typically encompass an employee benefit plan's trustees, administrators, investment managers and investment committee members. These standards of conduct require fiduciaries to (1) act solely in the interest of plan participants and their beneficiaries and with the exclusive purpose of providing benefits to them, (2) carry out their duties prudently, (3) follow the plan documents, unless

[1] For the first advisory, see An Overview of Cybersecurity Issues Affecting Retirement Plans and, for the second advisory, see Negotiating Cybersecurity Contractual Protections for Retirement Plans.

inconsistent with ERISA, (4) diversify plan investments and (5) pay only reasonable plan expenses. As discussed in further detail below, the duty to act prudently is one of a fiduciary's central responsibilities.

As ERISA imposes stringent penalties—most notably, personal liability—on fiduciaries who breach their duties, it is critical that fiduciaries clearly understand, and comply with, their duties under ERISA. However, in the context of cybersecurity, the lack of clarity surrounding such ERISA fiduciary duties can cause fiduciaries to breach their duties inadvertently.

Following is a discussion of ERISA fiduciary duties relating to cybersecurity and health and retirement plans, as well as best practices that ERISA fiduciaries should follow to maximize their compliance with such duties and to insulate their exposure to potential liability.

Health and Retirement Plans

ERISA group health plans with more than fifty participants or that are administered by a third party are subject to the regulations of the Department of Health & Human Services (HHS) concerning the privacy and security of protected health information (PHI) promulgated under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health or "HITECH" Act (together, HIPAA). As HIPAA-covered entities, these group health plans are required by the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of PHI maintained in electronic formats, protect against any reasonably anticipated threats or hazards to the security or integrity of that electronic PHI and uses or disclosures of that information that are not permitted under the HIPAA rules, and ensure compliance by its workforce. To comply with the HIPAA Security Rule, a covered entity, and each of its business associates, must perform a thorough and complete assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its electronic PHI and implement administrative, physical, and technical safeguards that reasonably and appropriately address that risk analysis. However, according to a recent fact sheet on ransomware and HIPAA published by HHS, entities are encouraged to implement additional and more stringent measures above what they determine to be required by the HIPAA Security Rule standards. For example, although there is not a HIPAA Security Rule standard that specifically requires entities to update the firmware[2] of network devices, entities—as part of their risk analysis and risk management process—should identify and address the risks to electronic PHI of using network devices running on obsolete firmware, especially when firmware updates are available to remediate known security vulnerabilities.

While the HIPAA rules thus contain specific requirements for addressing cybersecurity and group health plans, no equivalent law or set of regulations exists that governs cybersecurity and retirement plans. In addition, the Department of Labor is yet to issue formal guidance.

At the heart of the matter is the question of whether or not the responsibility to address cybersecurity issues is a fiduciary function. As discussed in our first client advisory, due to the perennial nature of cyberattacks, it may be difficult to argue that a prudent fiduciary would not consider and react to cyber risks. For this reason, retirement plan administrators and other fiduciaries should be cautioned against viewing protection of plan assets and participant information solely as the responsibility of external plan trustees and third party administrators. The agreements governing the provision of trustee and plan administrative services typically do not protect the plan fiduciaries even where the cybersecurity breach is

[2] Firmware refers to computer programs and data stored in hardware such that the programs and data cannot be dynamically written or modified during execution of the programs.

on the service provider's systems. In addition, as discussed below, ERISA fiduciaries cannot assume that their state privacy law duties will be preempted by ERISA.

Accordingly, plan fiduciaries should consider taking the following actions:

- review the agreements with plan administrators and providers as to the allocation of liability in the event of a cyber attack,
- assure that the plan sponsor has implemented a review of its own technology applicable to data stored and transferred relating to plan participants and plan investments, and that the plan sponsor has addressed any issues arising from such a review, and
- educate internal personnel as to how to communicate with participants in the event of a cyber attack.

ERISA and State Privacy and Data Laws

Nearly all U.S. states have enacted privacy and data laws, and these laws are not uniform. Under HIPAA, the privacy rule provides a Federal floor of privacy protections for PHI where such PHI is held by a covered entity or by a business associate. State laws that are contrary to the HIPAA privacy rules are generally preempted by the Federal requirements unless, for example, the state privacy law provides greater protections than the Federal law with respect to PHI. Those state laws will apply on their own terms with respect to personally identifiable information (PII) that is not PHI, for example, personal financial information that does not relate to health care or payment for health care.

Although ERISA's preemption of state laws is well-established, the extent to which ERISA preempts state privacy and data laws is less clear. In *Smilow, et. al. v. Anthem Life & Disability Ins. Co., et al*., No. 15-MD-02617-LHK (N.D. Cal. Nov. 24, 2015)—a case brought against Anthem by plaintiffs alleging that their PHI was compromised as a result of *Anthem's* massive data breach in December 2014—the Ninth Circuit followed the two-prong test established in *Aetna Health Inc. v. Davila*, 542 U.S. 200 (2004) in determining whether ERISA preemption applied. Under the test, ERISA preempts state law if:

1. the plaintiffs could have brought the claim under Section 502(a) of ERISA;[3] and
2. there is no other independent legal duty implicated by the defendant's actions.

The discussion that follows focuses on the second prong of the test. In *Anthem*, the Ninth Circuit explained that state law duties are not independent of ERISA if interpretation of the plaintiffs' benefit plans forms an essential part of the plaintiffs' claim, and if the duties are based on an obligation under an ERISA plan and the state law duties would not exist if the ERISA plan did not exist. Relying on the defendants' benefits handbook provided to the plaintiffs, that required *Anthem* to comply with state privacy laws, the Ninth Circuit concluded that the second prong of the test was satisfied.[4]

In contrast to *Anthem*, in *Rose v. HealthComp Inc*., No. 1:15-cv-00619-SAB (E.D. Cal. Aug. 10, 2015), applying the same two-prong test, the Ninth Circuit held that the second prong of the test was not satisfied.

[3] Section 502(a) of ERISA permits civil claims by a participant or beneficiary to (a) recover benefits due to him or her under the plan, (b) enforce rights under the plan or (c) clarify his or her rights to future benefits under the plan.

[4] On January 27, 2016, the plaintiffs' motion for leave to file a motion for reconsideration of the Ninth Circuit's November 24, 2015 order was denied (*Smilow, et al. v. Anthem Life & Disability Ins. Co., et al*., No. 15-MD-02617-LHK (N.D. Cal. Jan. 27, 2016)).

In *Rose*, the plaintiff's employment was terminated by her employer shortly after her employer received a copy of her medical records from the defendant. In considering whether the second prong had been satisfied, the Ninth Circuit used a "but for" test. Under such test, preemption exists if the state law cause of action would remain "but for" the denial of the claim for benefits. The Ninth Circuit found that, because the plan administrator's duty to safeguard the plaintiff's privacy under the California Constitution was independent from its obligations under ERISA, the claim did not meet the "but for" test and, therefore, there was an independent legal duty implicated by the cause of action.

These two cases demonstrate that whether ERISA preempts state privacy and data laws is hinged on the facts and circumstances. Accordingly, ERISA fiduciaries should not disregard state laws in developing and implementing their cyber risk management strategies. This is a newly-developing area of the law, and we will continue to monitor developments in the Ninth Circuit and other Circuits.

Best Practices

It is often challenging for fiduciaries to navigate their cybersecurity-related duties under ERISA. Therefore, to maximize compliance with their duties and minimize their exposure under ERISA, we recommend that fiduciaries of health and retirement plans:

1. Develop and implement a prudent cyber risk management strategy, as a part of a retirement plan's compliance program with ERISA and a group health plan's compliance program with HIPAA to address applicable state privacy and data breach notification laws. For example, this could include discussions and related diligence with the plan sponsor and legal counsel regarding protection of participant data and plan investment information stored on the plan sponsor's computer network or transferred to a third party provider, as well as documenting such compliance program.

2. Review existing plan documents to understand obligations in the event of a cybersecurity threat and breach, and engage third party administrators to confirm the parties' understanding of such obligations.

3. Develop a clear communication plan for notifying participants and beneficiaries of cybersecurity threats and attacks, including educating and training internal personnel (including the HIPAA security official and privacy official) and complying with HIPAA and applicable state privacy and data breach notification laws.

4. Consider all aspects of risk management, such as insurance coverage, including the level of coverage under their fiduciary liability insurance to ensure that they are adequately protected, as well as allocation of liability in underlying contractual arrangements with plan vendors.

If you have any questions about the content of this Advisory, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Susan P. Serota (bio)
New York
+1.212.858.1125
susan.serota@pillsburylaw.com

Christine L. Richardson (bio)
San Francisco
+1.415.983.1826
crichardson@pillsburylaw.com

Allen Briskin (bio)
Los Angeles
+1.213.488.7167
allen.briskin@pillsburylaw.com

Jessica Lutrin (bio)
New York
+1.212.858.1090
jessica.lutrin@pillsburylaw.com