

HIPAA Privacy,
Security, and Liability

By Elizabeth Doolin

Understanding HIPAA's privacy protections, and the potential exposure for violating them, is vital for any ERISA-governed health plan and its antecedents.

What Health Plans and Their Fiduciaries Need to Know

Stolen laptops. Old X-ray films. Discarded photocopiers. Decommissioned servers. Bankers boxes. What do these things have in common? They have all led to unauthorized disclosure of individuals' private health information,

along with substantial monetary penalties and increased regulatory scrutiny for the health-care entities involved.

While malicious data hacks take center stage in the news, a variety of less "newsworthy" situations can trigger legal exposure for violations of the privacy and security protections of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Office of Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) enforces HIPAA's privacy and security requirements, and the OCR has been aggressive in investigating complaints of HIPAA privacy violations, enforcing compliance with HIPAA's rules, and collecting millions in monetary penalties.

Private litigants have also sought redress for unauthorized disclosure of private health information, using HIPAA's requirements to season common law tort claims.

And for health insurers, health plans, and associated fiduciaries and business associates, the Employee Retirement Income Security Act (ERISA) potentially provides a basis for claims arising out of privacy breaches. Understanding HIPAA's privacy protections, and the potential exposure for violating them, is vital for any ERISA-governed health plan and its antecedents.

Overview of the HIPAA Privacy and Security Rules

HIPAA includes a set of specific standards to protect the privacy of patients' medical records and other health information (the Privacy Rule) and the security of protected health information held or transferred in electronic form (the Security Rule). Contained in the HHS HIPAA Administrative Simplification Regulations, 45 C.F.R. Parts 160, 162, and 164, the Privacy Rule and the Security Rule, along with the Enforce-



■ Elizabeth Doolin is a member of Chittenden Murday & Novotny LLC in Chicago. She has nearly 25 years of experience representing insurance and financial services industry clients in ERISA litigation, life insurance litigation, insurance coverage disputes, healthcare contract litigation, insurance tax litigation, commercial disputes, securities fraud and RICO claims, employment discrimination matters, and regulatory issues. Ms. Doolin has significant trial and appellate experience, and she is a frequent author and speaker on insurance and litigation issues. She has also been recognized as one of the Top 10 Women Civil Appellate Lawyers in Illinois by the Leading Lawyers Network. She is a member of the DRI Life, Health, and Disability, Data Management and Security, and Women in the Law Committees.

ment Rule, and the Breach Notification Rule, work together to implement the provisions of HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act of 2008 (GINA).

These rules are all contained in the “Omnibus Rule.” Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013). The Omnibus Rule was effective March 26, 2013, with full compliance required by September 23, 2013. The Privacy Rule can be found at 45 C.F.R. Part 160 and Part 164, Subparts A and E, while the Security Rule can be found at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

The major goal of the Privacy Rule and the Security Rule is “to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being.” U.S. Dep’t of Health and Human Servs., *Summary of the HIPAA Privacy Rule*, <http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>.

The Privacy and Security Rules protect all “individually identifiable health information” (“protected health information” or PHI) held or transmitted by a covered entity or a business associate, whether in paper, electronic or oral form. 45 C.F.R. §160.103. PHI includes information, including demographic data, that identifies or can be used to identify an individual and that relates to (1) an individual’s past, present, or future medical condition; (2) the provision of health care provided to that individual; or (3) the past, present, or future payment for the provision of health care to the individual. 45 C.F.R. §160.103.

Who Must Adhere to the HIPAA Privacy and Security Rules?

The Privacy and Security Rules define “covered entities” as health plans, health care clearinghouses, and any health-care provider who transmits any health information in electronic form. 45 C.F.R. §160.102(a) and 103. Health plans include individual and group plans that provide or pay the cost of medical care, including employer-sponsored group health plans,

government and church-sponsored health plans, and multi-employer plans. (The Privacy and Security Rules exclude group health plans that are both self-insured and self-administered and have less than 50 participants.) Health plans that must adhere to the Privacy and Security Rules also expressly include health insurance issuers and HMOs. 45 C.F.R. §160.103.

The Privacy and Security Rules also apply to “business associates,” 45 C.F.R. §160.102(b), which are defined as third parties that provide services to covered entities, including “claims processing or administration, data analysis, processing or administration, utilization review, quality assurance... billing, benefit management, practice management and repricing” as well as “legal, actuarial, accounting, consulting, data aggregation... management, accreditation, or financial services.” 45 C.F.R. §160.103.

Entities that provide data transmission services, as well as any person which “offers a personal health record to one or more individuals on behalf of a covered entity” and any subcontractor that “creates, receives, maintains, or transmits” PHI are also business associates under the Privacy and Security Rules. *Id.* Covered entities must ensure protections for PHI in a written agreement (termed the “business associate agreement”) with the business associates that it uses, which is to include express and specific written safeguards on the PHI used or disclosed by the business associate. 45 C.F.R. §164.504. Business associates that rely on subcontractors as additional business associates are in turn required to use written agreements that protect PHI. *Id.*

Moreover, the Omnibus Rule makes clear that business associates are directly liable for compliance with the requirements of the Security Rule, including all of its administrative, physical, and technical safeguards. 45 C.F.R. §164.302. Business associates must also ensure that the entities with which they subcontract comply with the Security Rule, and business associates are required to notify the covered entity for which they are providing services if a breach of unprotected PHI is discovered. Finally, business associates, as well as covered entities, are liable for civil monetary penalties under the Rules. 45 C.F.R. §160.102, 160.400.

What Do the HIPAA Privacy and Security Rules Require?

The HIPAA Privacy and Security Rules specifically require covered entities and business associates, among other things, to develop and to implement written privacy policies and procedures, 45 C.F.R. §164.530(i), and workforce privacy training, 45 C.F.R. §164.530(e), as well as appro-

The major goal of the Privacy Rule and the Security Rule is “to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being.”

priate safeguards to prevent the intentional and unintentional use or disclosure of PHI in violation of the Privacy Rule. 45 C.F.R. §164.530(f). The Privacy and Security Rules also include documentation and record retention requirements. 45 C.F.R. §164.530(j).

With respect to PHI that is created, received, maintained, or transmitted electronically (e-PHI), the Security Rule requires that covered entities and business associates must (1) ensure the confidentiality, integrity, and availability of e-PHI; (2) identify and protect against threats to the security of e-PHI; (3) protect against reasonably anticipated impermissible uses and disclosures of e-PHI; and (4) ensure compliance by their workforce with the requirements of the Security Rule. 45 C.F.R. §164.306(a).



The Omnibus Rule also updated the breach notification requirements for covered entities and business associates, codified at 45 C.F.R. Part 164, Subpart D, and applied to all breaches of PHI occurring after September 23, 2009. 45 C.F.R. §164.400. This “Breach Notification Rule” defines a breach as the “acquisition, access, use or disclosure of protected health infor-

and (3) the Secretary of HHS (for breaches involving 500 or more individuals), 45 C.F.R. §164.408(a). In addition, business associates must provide notification of a PHI breach to the applicable covered entity. 45 C.F.R. §164.410(a). Subpart D further provides detailed instructions for the manner, timing, and content of such required notifications.

lations due to “reasonable cause” and not willful neglect; (3) violations due to “willful neglect” corrected within 30 days of the violation becoming known or should have become known; and (4) violations due to “willful neglect” not corrected within 30 days. 45 C.F.R. §160.404(b)(2)(iv). The penalties range as shown in Table 1.

The Omnibus Rule defines “reasonable cause” to mean “an act or omission... which a covered entity or business associate knew, or by exercising reasonable diligence would have known” violated the Privacy and Security Rules but when the covered entity or business associate did not act with “willful neglect.” 45 C.F.R. §160.401.

The HHS considers the OCR to have the authority to enforce the Breach Notification Rule, including the authority to impose civil monetary penalties for the underlying privacy violations that led to the breach itself.

What HIPAA Enforcement Powers Does the HHS Have?

The HHS considers the OCR to have the authority to enforce the Breach Notification Rule, including the authority to impose civil monetary penalties for the underlying privacy violations that led to the breach itself. See U.S. Dep’t of Health and Human Servs., *Enforcement Highlights*, <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html>. With respect to enforcement, the Omnibus Rule invigorated the enforcement powers of the HHS, allowing it to investigate complaints and enforce compliance with the requirements of the Privacy and Security Rules. 45 C.F.R. §160.306 and 308. The HHS also has the power to assess civil monetary penalties to both covered entities and business associates. 45 C.F.R. §160.402(a). Significantly, both covered entities and business associates can be held liable for violations by other business associates acting as their agents. 45 C.F.R. §160.402(c). Note as well that violations of the Privacy and Security Rules include any violation, not only a breach violation.

HIPAA Privacy and Security Enforcement and Liability Trends

In recent years, the HHS has been happy to flex its enforcement muscle at health insurers, health plans, and related business associates. In its April 2016 enforcement report, the agency disclosed that the OCR received over 132,559 HIPAA complaints, initiated over 887 compliance reviews, and resolved over 96 percent of those cases. Resolution nearly always includes corrective measures (monitoring, increased reporting, training, and more frequent required risk assessments), and the monetary settlements totaled over \$36,639,200. See U.S. Dep’t of Health and Human Servs., *Enforcement Highlights, supra* (then follow “Enforcement Highlights Archived by Month” hyperlink).

Significantly, most of the violations in these cases did not result from malicious hacks of company databases, but instead they involved more prosaic, and arguably preventable, violations. Examples include a small pharmacy that kept patient records in an unsecured, open container (settlement of \$125,000 plus development of required policies and procedures and staff training), and an orthopedic practice that provided X-ray films of over 17,300 patients to a ven-

mation in a manner not permitted under Subpart E of this part which compromises the security or privacy” of PHI. 45 C.F.R. §164.402. Notably, the Breach Notification Rule *presumes* that the “acquisition, access, use or disclosure of protected health information in a manner not permitted under Subpart E” is a breach unless the covered entity or business associate “demonstrates that there is a low probability” that the PHI has been compromised, based on a risk assessment that considers the PHI involved, to whom it was disclosed, whether the PHI was actually acquired or viewed, and the extent to which the risk has been mitigated. *Id.*

The Breach Notification Rule does provide certain safe harbor provisions for encrypted PHI. *Id.* Covered entities must provide notification of a breach to (1) individuals whose PHI has been, or is reasonably believed to have been compromised, 45 C.F.R. §164.404(a); (2) “prominent media outlets” serving the state or jurisdiction of the individuals involved (when the breach involves the PHI of more than 500 individuals), 45 C.F.R. §164.406(a);

Of greatest interest, the Omnibus Rule increased the amount of civil monetary penalties available to the HHS, with a scale of potential penalties depending on the nature of the violation. The categories include: (1) violations about which the covered entity or business associate did not know and would not have known in the exercise of reasonable diligence; (2) vio-

Table 1

Violation Type	Penalty Per Violation	Maximum for Identical Violation Per Year
Unknown	\$100 - \$50,000	\$1,500,000
Reasonable Cause	\$1000 - \$50,000	\$1,500,000
Willful – Corrected	\$10,000 - \$50,000	\$1,500,000
Willful – Not Corrected	\$50,000	\$1,500,000

dor for digitization, without obtaining the necessary business associates agreement to protect PHI (settlement of \$750,000 plus revisions of key policies and procedures). See U.S. Dep't of Health and Human Servs., HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records (Cornell Compliance Enforcement example), and \$750,000 Settlement Highlights the Need for HIPAA Business Associate Agreements (Raleigh Orthopedic Clinic bulletin), <http://www.hhs.gov>.

Bigger violations do make the news. Affinity Health Plan, Inc., entered into a \$1,215,780 settlement with the OCR after a CBS news investigation revealed that photocopiers leased by Affinity (and then purchased by CBS) contained confidential medical information on the hard drives. The OCR concluded that Affinity impermissibly disclosed PHI when it returned the copiers, with the hard drives unwiped, to the leasing agent. The OCR concluded that Affinity also failed to recognize the potential for such a breach in its risk assessments. See Press Release, U.S. Dep't of Health and Human Servs., HHS Settles with Health Plan in Photocopier Breach Case (Aug. 14, 2013).

PHI stored on unencrypted laptops stolen from employees, or from third parties with no business associates agreement, have resulted in some of the biggest settlements, ranging from \$1.9 million (QCA Health Plan, Inc. of Arkansas) to over \$3.9 million (Northwest Health, Inc.). See Press Release, U.S. Dep't of Health and Human Servs., Stolen Laptops Lead to Important HIPAA Settlements (Apr. 22, 2014); Press Release, U.S. Dep't of Health and Human Servs., Improper Disclosure of Research Participants' Protected Health Information Results in \$3.9 Million HIPAA Settlement (Mar. 17, 2016).

The technical issues that can dog large-scale health-care operations play a part as well. Wellpoint Inc. paid \$1.7 million to the HHS in connection with a data breach resulting from security weaknesses in an online application database, while New York Presbyterian Hospital and Columbia University paid a combined \$4.8 million after PHI was compromised when a physician tried to deactivate a personal server connected to a shared network. See Press Release, U.S. Dep't of Health and Human Servs., WellPoint Pays HHS \$1.7 Million for

Leaving Information Accessible Over Internet (July 11, 2013); Press Release, U.S. Dep't of Health and Human Servs., Data Breach Results in \$4.8 Million HIPAA Settlements (May 7, 2014). All of these reported settlements highlight the importance to health plans and their business associates of the requirements of HIPAA's privacy and security Rules.

For health insurers, health plans, and related business associates, such OCR settlements or the imposition of civil monetary penalties are not the only potential source of liability for HIPAA privacy and security violations. In recent years, individuals seeking damages for unauthorized disclosure of PHI are turning to the courts. HIPAA's lack of a private right of action is no longer a shield from liability in these cases. In addition to state law tort claims, courts are recognizing potential ERISA-based claims related to unauthorized disclosure of their PHI, with HIPAA's Privacy and Security Rules providing a backdrop for such claims.

Shortly after Congress enacted HIPAA, the courts began to rule, consistently that the statute does not provide a private right of action for individuals to seek redress for HIPAA violations. See, e.g., *Swift v. Lake Park High Sch. Dist.*, 2003 WL 22388878, at *4 (N.D. Ill. Oct. 21, 2003); *Logan v. Dept. of Veterans' Affairs*, 357 F. Supp. 2d 149, 155 (D.D.C. 2004); *Johnson v. Quander*, 370 F. Supp. 2d 79, 99-101 (D.D.C. 2005); *Bellikoff v. Eaton Vance Corp.*, 481 F.3d 110, 116 (2d Cir. 2007); *Acara v. Banks*, 470 F.3d 569, 571 (5th Cir. 2006); *Webb v. Smart Document Solutions, LLC*, 499 F.3d 1078, 1081 (9th Cir. 2007) ("HIPAA itself provides no private right of action.").

For ERISA-governed health plans and their related business associates, however, these cases should not provide a false sense of security. Many decisions that acknowledge this general rule go on to recognize other avenues through which private litigants can seek redress, including ERISA.

As early as 1999, at least one district court recognized that a litigant had a viable claim for alleged HIPAA violations, asserted under ERISA. In *Stang v. Clifton Gunderson Heath Care Plan*, 71 F. Supp. 2d 926 (W.D. Wis. 1999), the plaintiff brought a claim for injunctive relief, under Section 502(a)(3) of ERISA, arguing that the plan at issue improperly denied health-care cover-

age to his dependent son in violation of 29 U.S.C. §1182(a)(1), the non-discrimination provision of HIPAA, codified as a provision of ERISA. *Stang*, 71 F. Supp. 2d at 928.

The plan countered, in part, that it was entitled to summary judgment on the plaintiff's claim because HIPAA's non-discrimination provision provided that an "enforcement action" such as the plain-

■ ■ ■ ■ ■
Eight years later,
the Eighth Circuit also
recognized that HIPAA's
anti-discrimination provisions
can be enforced by a
plan participant's Section
502(a)(3) claim "to enjoin
any active practice which
violates any provision of the
subchapter." *Werdehausen
v. Benicorp Ins. Co.*, 487
F.3d 660 (8th Cir. 2007).

tiff's was premature under HIPAA. *Id.* at 932. The court pointed out, however, that a private right of action under ERISA, and not "enforcement" by the U.S. Department of Labor (DOL), was what the plaintiff sought, and thus the timing argument raised by the plan did not apply. In so ruling, the court recognized the viability of an ERISA claim to challenge a HIPAA violation in the context of HIPAA's non-discrimination provisions.

Eight years later, the Eighth Circuit also recognized that HIPAA's anti-discrimination provisions can be enforced by a plan participant's Section 502(a)(3) claim "to enjoin any active practice which violates any provision of the subchapter." *Werdehausen v. Benicorp Ins. Co.*, 487 F.3d 660 (8th Cir. 2007). While the court noted



that under the specific facts of that case, the plan had *not* violated HIPAA's anti-discrimination provisions, it went on to observe, "congressional intent underlying HIPAA is relevant to determining whether Benicorp's policy of automatic rescission breached its fiduciary duty as an ERISA benefits decision maker." 487 F.3d at 668.

The Eighth Circuit then offered that

Both the *Anthem*

decisions and the *Quintana* decision show that federal common law rejecting a private right of action for HIPAA violations is no protection for health plans, health insurers, and their business associates involved in a potential breach of PHI.

"HIPAA supplies a 'relevant rule of decision' for the Werdehausen's claim to recover benefits and enforce the terms of the plan under 29 U.S.C. Section 1132(a)(1)(B)." *Id.* While it was addressed in the context of HIPAA's anti-discrimination provisions, the *Werdehausen* court nevertheless linked a HIPAA violation to *both* a discrimination and an ERISA benefits claim.

Other courts have relied on the reasoning in *Stang* and *Werdehausen* to recognize that while HIPAA itself provides no private right of action, ERISA is a viable way to challenge a plan action that arguably violates HIPAA's anti-discrimination rules. See *E.L. v. Scottsdale Healthcare Corp. Plan*, 2011 WL 3489644, at*3 (D. Ariz. Aug. 9, 2011) (recognizing possible Section 502(a)(3) claim to address HIPAA violation); *Ames v. Group Health Inc.*, 53 F. Supp. 2d 187, 192 (E.D.N.Y. 2008) (recognizing possible Section 502(a)(3) claim to address HIPAA violation).

While these cases involve HIPAA's non-discrimination provisions, which are expressly codified in the ERISA statute, more recent decisions have dealt with claims of privacy violations and disclosure of PHI and recognized such claims as *either* potential ERISA claims, or as state common tort claims not preempted by ERISA. For example, in *In re Anthem, Inc. Data Breach Litigation*, 2015 WL 5286992, at*1 (N.D. Cal. Sept. 9, 2016), the court addressed a punitive class action for breach of contract and a variety of other state statutory and common law claims arising out of a cyberattack on the computer system of Anthem Inc. and the result in disclosure of individuals' PHI. In their complaint, the plaintiffs' alleged that PHI protected by HIPAA was compromised by the cyberattack. Certain defendants removed the case to federal court, arguing in part that ERISA provided federal question jurisdiction. *Id.* at *2.

In denying the plaintiffs' motion to remand, the court found that their state law contract claims arising out of the data breach and disclosure of PHI were completely preempted by ERISA, thus providing adequate federal jurisdiction. *Id.* at *5. The court pointed out, however, that the plaintiffs' complaint sought to enforce their rights under the terms of their respective ERISA plans, specifically with allegations that the plaintiffs' "agreements for services" with the defendants "included promises to secure, safeguard, protect, keep private, and not disclose Plaintiffs' and class members PHI." *Id.* at *4. Accordingly the court found that the plaintiffs' claims fell within the purview of Section 502(a)(1)(B) of ERISA. *Id.*

The plaintiffs argued that the contract to which they referred was the HIPAA Notice of Privacy Rights attached to their ERISA plans, and not the plans themselves. The court rejected this argument, concluding that "the 'agreement[s] for services' between the Defendants and Plaintiffs... are their employer-sponsored ERISA plans. The HIPAA notices accompanying those plans are therefore 'part of those 'agreement[s] for services' and not the agreements themselves." *Id.* See also *In Re Anthem Inc. Data Breach Litigation*, 2015 WL 7443779, at *5 (N.D.Cal. Nov. 24, 2015) (holding same with respect to different set of consolidated plaintiffs).

In contrast, the court rejected an ERISA preemption argument for state law tort claims (invasion of privacy, conspiracy to invade privacy, negligent infliction of emotional distress) arising out of a PHI privacy breach by a health plan's subrogation vendor in *Quintana v. Lightner*, 818 F. Supp. 2d 964 (N.D. Tex. 2011). In *Quintana*, the plaintiff claimed that his ERISA-governed health plan's subrogation vendor improperly disclosed his confidential PHI in connection with the plan's subrogation rights. *Id.* at 967. The vendor removed the case, arguing that the plaintiff's claims were preempted by ERISA. The court remanded the claims back to state court, finding that the breach of privacy tort claims were based on an "independent right to privacy." *Id.* at 971. The court also concluded that the invocation of HIPAA in the complaint was not enough independently to confer federal jurisdiction. *Id.*

Both the *Anthem* decisions and the *Quintana* decision show that federal common law rejecting a private right of action for HIPAA violations is no protection for health plans, health insurers, and their business associates involved in a potential breach of PHI. Claims against a health plan directly, or which can be characterized as enforcing plan rights (including privacy rights), are more likely to be preempted by ERISA, but they can still stand as potential claims to enforce plan rights under Section 502(a)(1)(B), bolstered by prior decisions recognizing the notion that HIPAA can supply the "rule of decision" for precisely what those privacy rights may be.

Conclusion

Whether ERISA plan fiduciaries may face additional ERISA liability in the form of "appropriate equitable relief" for violations of plan privacy rights remains to be seen, but is certainly not outside of the realm of possibility. See *CIGNA Corp. v. Amara*, 563 U.S. 421, 442 (2011) (recognizing possibility of surcharge as a form of equitable relief against a plan fiduciary). The prospect of ERISA or state law liability for HIPAA violations should be a real concern for ERISA-governed health plans and their fiduciaries. Having awareness of and complying with the HIPAA Privacy and Security Rules is essential.

