ERISA Enforcement of the HIPAA Privacy Rules

Jamie Lund†

Autoworker Daniel Duffey, an employee of General Motors Corporation (GM), took advantage of GM's Employee Assistance Program (EAP), which "provides counseling and related services for employees with problems such as those stemming from alcohol and drug abuse." As a participant in the program, Daniel revealed his status as a substance abuser. GM subsequently discharged him. When he filed a grievance protesting the discharge, allegations relating to his participation in the EAP began to circulate, despite previous written assurances of confidentiality. He sued GM, alleging violations of state privacy and contract laws. GM removed the case to a federal court, which dismissed Daniel's claims as preempted by the Employee Retirement Income Security Act (ERISA). According to the court, Daniel was required to proceed on a federal cause of action or none at all. Did Congress intend for Daniel to lose his state claims? If so, did Congress want him to have a federal cause of action, and under what circumstances?

Because ERISA broadly preempts many state privacy remedies without creating any of its own, parties like Daniel were left without any recourse for privacy violations. In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) to protect individually identifiable health information. As Daniel's case illustrates, one way to increase the protection of private health information would be to allow individual civil suits against violators of privacy rules like those established by HIPAA. However, HIPAA itself and the regulations adopted to implement its privacy protection contain no explicit private right of action, and courts have refused to infer a private cause of action under HIPAA for privacy violations.

† B.M. 2002, Brigham Young University; J.D. Candidate 2006, The University of Chicago.

1 This scenario is based on the facts and holding of In re General Motors Corp, 3 F3d 980, 982 (6th Cir 1993).

2 29 USC § 1001 et seq (2000).

3 General Motors, 3 F3d at 985.


6 See, for example, University of Colorado Hospital Authority v Denver Publishing Co, 340 F Supp 2d 1142, 1145 (D Colo 2004) ("[L]egal commentators appear to unanimously assume that there is no private right of action under HIPAA, including to enforce the 'privacy rule' of § 1320d-6."). See also Françoise Gilbert, Emerging Issues in Global AIDS Policy: Preserving Privacy, 25 Whittier L Rev 273, 289 (2003); Frederick Y. Yu, Medical Information Privacy Under
Another possible route for a private right of action for certain plaintiffs—if such an action should exist—could look to the intersection of HIPAA and ERISA. HIPAA requires ERISA plans to comply with HIPAA’s privacy rules and to amend or produce compliant documents. Thus, victims of privacy violations related to their ERISA-regulated healthcare plans could conceivably sue to enforce the privacy rules as “terms of the plan” under § 502(a) of ERISA.

This Comment discusses whether, despite the lack of a private cause of action under HIPAA itself, a private cause of action should be recognized under ERISA for HIPAA privacy-rule violations—whether such a cause of action is supported by the statutory language and legislative intent of both statutes, and if so, where it would originate. In doing so, the Comment addresses whether granting such a cause of action undermines the system of privacy regulations codified by HIPAA.

Part I gives a brief overview of both the HIPAA privacy rules and the ERISA private enforcement scheme. Part II addresses whether Congress intended to create any of the aforementioned private causes of action, and if so, which among them? In particular, Part II explores whether the statutory language and legislative history of ERISA and HIPAA support ERISA enforcement of HIPAA privacy rules. Part III first discusses statutory remedies generally and then explores the possibility that “terms of the plan” can come from sources other than the standard plan documents. Particularly, Part III examines whether ERISA document changes or additions enacted pursuant to HIPAA may embody terms of the plan. Finally, Part III explores whether pri-

7 HIPAA affects all ERISA plans that provide or pay for the cost of medical care, except self-insured plans that are administered by a sole employer and have fewer than fifty participants. 45 CFR §§ 160.103. See also Covered Entity Decision Tools: Is a Private Benefit Plan a Health Plan? online at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/xmldecision.asp?decision=D3 (visited Aug 17, 2005). Other covered entities include health insurance issuers, HMOs, and health care providers. Id at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp (visited Aug 17, 2005).

8 “Terms of the plan” is not defined by the statute, but courts generally interpret it to mean those rights and benefits conferred on participants as specified in the plan documents. See Part II.B.

9 The most commonly used ERISA private remedies, § 502(a)(1)(B), codified at 29 USC § 1132(a)(1)(B), and its equitable companion, § 502(a)(3), codified at 29 USC § 1132(a)(3), give participants and beneficiaries a private cause of action to recover benefits due or to enforce their rights under the terms of the plan.
privacy-rule plaintiffs can bring ERISA actions for breach of fiduciary duty. Ultimately, the Comment concludes that, despite the lack of any explicit manifestation of Congress’s intent to create an ERISA cause of action for HIPAA privacy-rule violations, the statutes interact in a way that implies such intent.

I. AN OVERVIEW OF HIPAA AND ERISA

The purpose of ERISA is to protect employees; the purpose of HIPAA is to protect individuals’ health information. As they are written, ERISA and HIPAA might interact in such a way that employees may sue for unauthorized use of their health records. This Part provides background on ERISA, HIPAA, and their interaction. Part I.A focuses on the privacy rules—what they are, whom they affect, and how they are enforced. It also discusses the elements of HIPAA that are possible candidates for ERISA enforcement—the amendments regarding disclosure to plan sponsors and the privacy notice. Part I.B discusses ERISA, its written requirement, and how it generally preempts state-law privacy claims without creating any privacy rights of its own.

A. HIPAA

Although HIPAA’s principal purpose is to increase access to healthcare through expanded portability and renewability of insurance, HIPAA also governs the use of individually identifiable health information. Its regulations took effect on April 14, 2003 (April 14, 2004, for smaller health plans).

1. Privacy rules.

HIPAA’s privacy rules are the primary means of federal regulation of health privacy. The privacy rules were issued by the Secretary of Health and Human Services (HHS) under his rulemaking authority. These rules provide individuals with new rights and regulate the

---

10 Health Insurance Portability and Accountability Act of 1996, HR Rep No 104-496, 104th Cong, 2d Sess 1 (1996), reprinted in 1996 USCCAN 1865 (reporting that HIPAA was enacted to “improve portability and continuity of health insurance coverage”).
12 See id § 164.534.
13 Smaller health plans include those with annual receipts of $5 million or less. 45 CFR § 160.103 (2004).
14 45 CFR §§ 164.500–164.534 (creating national standards regarding the confidentiality of individuals’ medical records and other personal health information).
15 The Secretary’s rulemaking authority was pursuant to Subtitle F, Title II of HIPAA, 110 Stat at 2021–31, codified at 42 USC § 1320d-2 (2000). For a discussion of the legitimacy of the privacy rules, see South Carolina Medical Association v Thompson, 327 F3d 346, 349–55 (4th Cir
ways in which "covered entities" can use or disclose protected health information. Most notably, the rules restrict unauthorized uses and disclosures of information related to nontreatment, nonpayment, and non-healthcare operations. The privacy rules protect information that is individually identifiable, which is any personally identifying information "created or received by a health care provider" that "relates to the ... health or condition of an individual" or to the provision of or payment for healthcare. For instance, an individual's HIV-positive status is protected health information, as is Daniel's participation in a substance abuse program.

HIPAA permits covered entities to use or disclose information in some circumstances, requires them to disclose information in others, and prohibits use or disclosure of information in still others. A covered entity may use and disclose protected health information for its own treatment, payment, and healthcare operations and may make limited disclosures to other entities for healthcare-operations activities, fraud and abuse detection, and compliance. However, the privacy rules permit covered entities to make only the minimum necessary disclosures.

2003) (concluding that HIPAA did not violate the nondelegation doctrine, that the promulgated rules do not exceed the statutory authorization, and that the "non-preemption" provision was not impermissibly vague); Assn of Am Physicians & Surgeons v United States Dept of Health and Human Services, 224 F Supp 2d 1115, 1126–29 (SD Tex 2002), affd, 67 Fed Appx 253 (5th Cir 2003) (concluding that regulations did not exceed statutory framework and that the Department of Health and Human Services (HHS) took the proper procedural steps in promulgating the rules).

A covered entity is essentially any healthcare provider (for example, a hospital) or insurer (for example, an HMO) that transmits health information electronically, including all ERISA plans except self-insured plans that are administered by employers and have fewer than fifty participants. 45 CFR §§ 160.102–160.103 (2004).

Protected Health Information means individually identifiable health information that is “(i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium,” but excludes individually identifiable health information in “(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.” 45 CFR § 160.103(1)–(2).

45 CFR § 164.502(a).

For a discussion about the particular needs of AIDS/HIV confidentiality, see Gilbert, 25 Whittier L Rev at 278–79 (cited in note 6).

Id § 164.506(c).

Id § 164.502(b)(1).
In addition, HIPAA requires covered entities to disclose information in two circumstances: (1) when an individual or his personal representative requests access to the individual's personal health information, and (2) when HHS requests such information as part of a compliance investigation or review. All other disclosures require the covered individual's written authorization. By strictly regulating the disclosures of personally identifying health information, the rules ensure the privacy of individuals' health information.

2. Amendments for disclosures to plan sponsor.

The privacy rules require ERISA plan sponsors to create or alter documents, including amending plan documents to restrict disclosure of health information to plan sponsors. The regulation provides that "a group health plan, in order to disclose protected health information to the plan sponsor . . . must ensure that the plan documents restrict the uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart." Proper disclosures include whether an individual participates in the health plan, summary health information for use in obtaining bids from providers, and information necessary for administrative functions.

3. Notice of privacy practices.

HIPAA requires ERISA plan sponsors to provide plan participants with documents detailing parties' rights and obligations under HIPAA, including the "privacy notice." Each covered entity that cre-
ates or receives protected health information must create and maintain a “Notice of Privacy Practices” detailing potential uses and disclosures of protected health information. Although there are special exemptions for group health plans, such plans are still required to provide privacy notices if they do not provide health benefits through an independent insurance provider or health maintenance organization (HMO)—that is, if they are self-insured. Additionally, group health plans that are not self-insured but create or receive protected health information must maintain privacy notices and provide such notices upon request to any person.

Privacy notices must thoroughly communicate and represent participants’ rights and administrators’ duties. In fact, the stated purpose of a privacy notice is to describe to the participant how medical information may be used and disclosed and how the participant can access such information. The privacy notice must be written in “plain language,” include at least one example of the types of uses and disclosures permitted, and detail all intended uses and disclosures that may be made without the individual’s consent. The notice must also include a description of any disclosures that the plan intends to make to the plan sponsor. Moreover, as a catchall, the notice must state that no other uses and disclosures may be made without the individ-

(2) ... (i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO;...

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information ... or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and
(B) Provide such notice upon request to any person.

Id § 164.520(a).

33 Id § 164.520(b)(1)(ii). Covered entities include all ERISA plans except self-insured plans that are administered by employers and have fewer than fifty participants. Id § 160.102–160.103.

34 Id § 164.520(a)(2)(i). Self-insured plans were required to provide these notices to all participants by the compliance date. Id § 164.520(c)(2)(i)(A). New enrollees must be given a copy of the notice upon enrollment and a reminder every three years that the notice is available upon request. Id § 164.520(c)(1).

35 Id § 164.520(a)(2)(ii).

36 Id § 164.520(b).

37 Id § 164.520(b)(1)(i).

38 Id § 164.520(b)(1)(ii)(A)–(B).

39 Id § 164.520(b)(1)(iii)(C).
ual's written authorization and that the individual may revoke such authorization at any time.40

No court has considered whether privacy notices can be privately enforced under ERISA. This Comment argues that the notices are meant to be clear and representative of participants' rights and administrator's duties and thus can and should serve as bases for suits under ERISA.

4. Enforcement.

Although the privacy rules are designed to protect individuals' private health information,41 Congress created no independent private cause of action for privacy-rule violations. Instead, Congress provided a public enforcement scheme that imposes penalties, including fines and criminal punishment, for violations of the privacy rules.42 HHS's Office of Civil Rights (OCR) enforces the privacy rules through a complaint-driven process.43 OCR is required "to make sure that consumers receive the privacy rights and protections required under the new regulations."44 OCR can impose fines of up to $100 per knowing failure to comply with a privacy-rule provision, not to exceed $25,000 per year for multiple violations of the same requirements.45 In addition to assigning penalties, OCR can refer potential criminal violations to

40 Id § 164.520(b)(ii)(E). Other rights specified in the privacy notice include the right to request additional restrictions with regard to health information; the right to request confidential communications from the health plan; the right to inspect, copy, and amend personal health information; and the right to receive an accounting of health information disclosures and a copy of the privacy notice upon request. Id § 164.520(b)(1)(iv).

Today's 4th Circuit ruling upholding the constitutionality of the HIPAA Privacy Rule [South Carolina Medical Association, 327 F3d 346] is a victory for America's patients and the principle that the federal government can provide protections to insure [sic] the enhanced confidentiality of their medical records.

This administration strongly supports a policy of providing a first-time-ever federal level of protection for the medical records of all Americans. The rule helps to ensure appropriate privacy safeguards are in place as we harness information technologies to improve the quality of care provided to patients. Consumers will benefit from these new limits on the way their personal medical records may be used or disclosed by those entrusted with this sensitive information.

43 45 CFR §§ 160.300–160.312.
44 HHS, Fact Sheet (cited in note 42). See also 45 CFR § 704.2 (stating that "[a]ny person may bring to the attention of the Commission a grievance that he or she believes falls within the jurisdiction of the Commission" via a written complaint submitted to the Office of Civil Rights Evaluation).
the Department of Justice for further investigation and appropriate action.46

It is still too early to determine how well these enforcement methods work, but there is some suggestion of underenforcement. Surprisingly few complaints were filed in the first year that the privacy rules were effective, and no fines or criminal penalties were assessed that year.47 This apparent lack of enforcement could be OCR’s response to the health industry’s concerns that enforcement would be heavy-handed48 or could perhaps be due to a lack of funding. OCR has a reputation for being “toothless,”49 and some insiders opine that OCR will not successfully enforce HIPAA.50

Especially troubling is HIPAA’s apparent lack of protection in the workplace. Because employers are generally not covered entities, complaints by employees that their health information has become “the talk of the workplace” are beyond the jurisdiction of OCR to investigate.51 Moreover, state-law privacy claims are often preempted by ERISA in employment situations.52 However, this Comment argues that health information created as a result of an employee health plan can be protected against unauthorized employer access and disclosure through ERISA.

Additionally, although HIPAA’s civil and criminal enforcement provisions should deter most violators, HIPAA contains no compensation provisions for the victims of privacy violations.53 Under HIPAA, victims can only file written complaints, which may spark public en-

46 Id; Robin A. Johnson, Administrative Simplification Provisions of HIPAA, Mass Health & Hospital Law 9-1 (2004) (“The statute establishes civil money penalties and criminal penalties for violations. . . . HHS will enforce the civil money penalties, while the U.S. Department of Justice will enforce the criminal penalties.”) (internal citations omitted), citing 42 USC § 1320d-5; HHS, Standards for Privacy of Individually Identifiable Health Information, 65 Fed Reg 82461-2-01 at 82472 (“OCR will be responsible for enforcement of this regulation [including] investigating complaints and conducting compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution.”).


49 HIPAA Compliance Strategies (cited in note 47).

50 Id (“An insider with close ties to government says as long as OCR is in charge, ‘I don’t think you’ll have successful HIPAA enforcement.’”).

51 Id.

52 See the discussion of ERISA preemption in Part I.B.2.

53 This aspect of the privacy rules was criticized in Sarah Lai Stirland, Privacy: Group Blasts Enforcement of Healthcare Privacy Rules, Natl J Tech Daily (Apr 12, 2004, PM ed) (quoting the president of the Institute for Health Freedom as saying, “They’ve only been given the right to complain, period. . . . We should have a law that’s consumer, or citizen, driven.”).
ERISA Enforcement of the HIPAA Privacy Rules

For instance, if Daniel suspects that he was fired because GM improperly accessed private health information related to his treatment, he can file a complaint, which might lead to an investigation. As a result of the investigation, OCR could fine GM or refer GM officials who accessed Daniel's private information to the Department of Justice for possible prosecution and imprisonment. But the OCR enforcement process would not restore Daniel's job; HIPAA does not authorize the OCR or the Department of Justice to impose any remedy or punishment other than those fines and criminal sentences specified in 42 USC § 1320d-6, and at least one court has refused to enjoin a privacy-rule violation.

B. ERISA

Congress enacted ERISA primarily to protect the interests of participants in and beneficiaries of employee benefit welfare plans by establishing standards of conduct, responsibility, and obligation for fiduciaries and by providing appropriate remedies and access to federal courts.

1. Written requirement.

A plan sponsor is required to establish and maintain a plan in accordance with a written document. Courts will focus on the written plan document when examining the terms of the plan. However, as the

---

54 See 45 CFR § 704.2.
55 Perhaps recognizing this potential weakness in the HIPAA enforcement structure, at least one court has opted to enforce the privacy rules under other federal regulations, specifically, the discovery rules of the Federal Rules of Civil Procedure. For a discussion of Law v Zuckerman, 307 F Supp 2d 705 (SD Md 2004), see Part III.A.2.
56 University of Colorado Hospital Authority v Denver Publishing Co, 340 F Supp 2d 1142, 1143-46 (D Colo 2004) (rejecting a hospital's request to enjoin the publication of protected health information because HIPAA has no independent cause of action).
57 A welfare plan is any plan, fund, or program... established or maintained by an employer or by an employee organization, or by both,... for the purpose of providing its participants or their beneficiaries [with certain benefits]. [These include] medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, death, or unemployment.
29 USC § 1002(1).
59 Employee welfare benefit plans are established by employers and/or employer unions who are known as plan sponsors. 29 USC § 1002(1).
60 29 USC § 1102(a)(1).
61 See In re Unisys Corp Retiree Medical Benefit "ERISA" Litigation, 58 F3d 896, 902 (3d Cir 1995) ("A court must examine the plan documents."); Biggers v Wittek Industries, 4 F3d 291, 295 (4th Cir 1993) ("A written plan is critical to ERISA's goal that employees be informed about the benefits to which they are entitled. Oral or informal written amendments are inadequate to alter the written terms of a plan, as this practice would undermine certainty."). See also Cinnelli v
Eleventh Circuit pointed out in Donovan v Dillingham,\textsuperscript{62} "it would be incongruous for persons establishing or maintaining informal or unwritten employee benefit plans . . . to circumvent the Act merely because an administrator or other fiduciary failed to satisfy reporting or fiduciary standards."\textsuperscript{63} Most courts have similarly held that a plan may exist even in the absence of a written document.\textsuperscript{64} Also, as discussed in Part II.A.2, most courts hold that some aspects of a plan may be ascertained from sources other than the official written plan document.

2. ERISA preemption.

As evidenced by Daniel Duffy's case, ERISA contains a very broad preemption clause that can preempt state privacy laws insofar as they pertain to employee health benefits.\textsuperscript{65} ERISA preempts, with few exceptions, "any and all State laws insofar as they may now or hereafter relate," either directly or indirectly, "to any employee benefit plan."\textsuperscript{66} Courts have traditionally held this provision to preempt almost every type of claim that tangentially touches upon an ERISA-regulated health plan, in order to promote the preemption clause's purposes: eliminating conflicting and inconsistent state laws and freeing plan administrators from the burden of having to conform to more than one set of laws and standards.\textsuperscript{67}

The Supreme Court retreated from its original expansive interpretation of ERISA preemption in New York State Conference of Blue Cross & Blue Shield Plans v Travelers Insurance Co\textsuperscript{68} by stating that "preemption does not occur . . . if the state law has only a tenuous, remote, or peripheral connection with covered plans."\textsuperscript{69} However, the

\textsuperscript{62} Security Pacific Corp, 61 F3d 1437, 1444 (9th Cir 1995) (noting that claims for estoppel cannot contradict the written terms of the plan).
\textsuperscript{63} 688 F2d 1367 (11th Cir 1982) (en banc).
\textsuperscript{64} Id at 1372.
\textsuperscript{65} For a complete listing by circuit, see Jayne E. Zanglein and Susan J. Stabile, ERISA Litigation 7 (BNA Books 2003).
\textsuperscript{66} See In re General Motors Corp, 3 F3d 980, 985 (6th Cir 1993) (holding that the plaintiffs' state privacy claims for the employer's alleged access to health files were preempted by ERISA).
\textsuperscript{67} See also Nathalie Smith, Note, The Right to Genetic Privacy? Are We Unlocking the Secrets of the Human Genome Only to Risk Insurance and Employment Discrimination?, 2000 Utah L Rev 705, 745-56 (discussing the policy behind proposed Utah state legislation restricting the use of private health information in employment contexts).
\textsuperscript{68} 29 USC § 1144.
\textsuperscript{69} See 120 Cong Rec H 29197 (Aug 20, 1974) (statement of Rep Dent) (asserting that preemption protects "participants by eliminating the threat of conflicting and inconsistent State and local regulation").
Court’s recent decision in *Aetna Health Inc v Davila* suggests that ERISA preemption is still broad. Furthermore, lower court decisions continue to include broad preemption language. For example, the Sixth Circuit, while acknowledging certain exceptions to ERISA preemption doctrine, has “repeatedly recognized that virtually all state law claims relating to an employee benefit plan are preempted by ERISA.”

Although ERISA itself does not contain health privacy regulations, courts have sometimes held that ERISA preempts state-created private causes of action for privacy violations, leaving plaintiffs without a viable state or federal cause of action. This “regulatory vacuum” was criticized by Justice Ginsburg in her *Davila* concurrence. Although Justice Ginsburg agreed with the majority that upholding ERISA preemption was consistent with governing case law, she asserted that the Court’s “encompassing interpretation of ERISA’s preemptive force” coupled with “a cramped construction of the ‘equitable relief allowable under § 502(a)(3)” creates a “regulatory vacuum” in which “[v]irtually all state law remedies are preempted but very few federal substitutes are provided.”

The problem that Justice Ginsburg notes is illustrated by Daniel’s dilemma. Daniel originally brought his claim under a state privacy law, but the federal court held that GM’s Employee Assistance Program was an employee welfare benefit plan for purposes of ERISA and, accordingly, that ERISA preempted Daniel’s state privacy and breach of confidentiality claims. Because ERISA has been held to preempt state-law privacy claims without creating any of its own, plaintiffs like Daniel have either a federal cause of action or none at all.

In contrast, other courts have construed ERISA’s preemption clause to be less inclusive when dealing with state-law health privacy claims. For instance, the Fourth Circuit has held that claims regarding the confidentiality of medical records are not preempted when the offenses by the ERISA plan administrator are unrelated to the administrator’s duties under the plan. Likewise, the Ninth Circuit, in a case

---

70 124 S Ct 2488 (2004).
71 Id at 2495–96.
72 *Marks v Newcourt Credit Group, Inc*, 342 F3d 444, 452 (6th Cir 2003).
73 See, for example, *In re General Motors*, 3 F3d at 985.
74 *Davila*, 124 S Ct at 2503 (Ginsburg concurring) (“I also join the rising judicial chorus suggesting that Congress and [this] Court revisit what is an unjust and increasingly tangled ERISA regime.”) (internal quotation marks omitted), quoting *DiFelice v Aetna U.S. Healthcare*, 346 F3d 442, 453 (3d Cir 2003) (Becker concurring).
75 *In re General Motors*, 3 F3d at 985.
76 See *Darcangelo v Verizon Communications, Inc*, 292 F3d 181, 194 (4th Cir 2002). See also *Duchesne-Baker v Extendicare Health Services, Inc*, 2003 US Dist LEXIS 18168, *21 (ED La) (“ERISA does not provide a cause of action to participants or beneficiaries for a plan administrator’s tortious acts that are unrelated to his duties pursuant to its administration of the ERISA plan.”).
involving a claim for tortious invasion of privacy, concluded that restric-
tions such as those prohibiting administrators from hiring private
investigators do not conflict with the purpose behind ERISA preemp-
tion—not to hold administrators accountable for fifty different sets of
rules for plan administration. 7

The critical question for these courts seems to be this: how closely
does the state-law or tort claim “mandate employee benefit structures
or their administration”? 8 The lesser the impact upon such structures
and administration, the less likely the state law is to be preempted
by ERISA. 9 In the tortious invasion of privacy case described above, for
example, the plaintiff alleged that the investigators acquired personal
information about him by impersonating him. 80 The Ninth Circuit sug-

The critical question for these courts seems to be this: how closely
does the state-law or tort claim “mandate employee benefit structures
or their administration”? 7 The lesser the impact upon such structures
and administration, the less likely the state law is to be preempted
by ERISA. 9 In the tortious invasion of privacy case described above, for
example, the plaintiff alleged that the investigators acquired personal
information about him by impersonating him. 80 The Ninth Circuit sug-
gested that ERISA should not preempt any and every state tort claim:
“Making ERISA administrators liable for investigations perpetrated
by their agents which would be objectionable or offensive to the rea-
sonable man simply cannot be said to interfere with nationally uni-
form plan administration.” 81

Despite the more lenient approach adopted by some courts, how-
ever, the enactment of HIPAA may have rendered ERISA preemp-
tion of health privacy claims more likely. Health privacy was never a
“federal concern” before HIPAA, but the enactment of HIPAA has
made health privacy protection part of the administrative duties of
ERISA plan administrators. To the extent that state privacy laws or
tort actions interfere with the HIPAA privacy standards, then, ERISA
might preempt them.

Although the “amorphous contours of the preemption doctrine” 82
make it difficult to predict when ERISA will preempt state laws,
ERISA still preempts many state private remedies for patient confi-
dentiality violations. 83 This is probably even truer after the enactment

77 Dishman v UNUM Life Insurance Co of America, 269 F3d 974, 981–82 (9th Cir 2001).
78 Travelers, 514 US at 646.
79 Brian A. Pérez-Daple, Comment, Legal Reimbursement Claims by ERISA Plan Fiduci-
80 Dishman, 269 F3d at 979.
81 Id at 982 (internal quotation marks omitted).
82 Id at 980. See also Egelhoff v Egelhoff, 532 US 141, 152–53 (2001) (Scalia concurring) (“I
remain unsure (as I think the lower courts and everyone else will be) as to what else triggers the
‘relate to’ provision.”).
83 See Smith, Note, 2000 Utah L Rev at 734 (cited in note 65) (recognizing that although
ERISA itself does not contain provisions for the protection of patient confidentiality and pri-
vacy, state privacy remedies against self-insured employers are often preempted by ERISA);
Cynthia Stamer, Invasion of Medical Privacy, in Zanglein and Stabile, ERISA Litigation at 797–
808 (cited in note 64) (acknowledging the trend toward preempting state privacy law claims but
arguing that the trend may be reversing).
of HIPAA. Thus, a federal cause of action for HIPAA privacy-rule violations may be the only recourse available to private plaintiffs.\footnote{See \textit{Bast v Prudential Insurance Co of America}, 150 F3d 1003, 1010 (9th Cir 1998) (holding that ERISA preempts state-law claims, even if the result is that a claimant, relegated to asserting a claim only under ERISA, is left without a remedy); \textit{Cromwell v Equicor-Equitable HCA Corp}, 944 F2d 1272, 1276 (6th Cir 1991) ("Nor is it relevant to an analysis of the scope of federal preemption that appellants may be left without a remedy.").}

Having established that there is no independent cause of action under HIPAA and that ERISA preempts at least some state privacy causes of action, it is important to examine how ERISA and HIPAA interact to determine whether a privacy cause of action through ERISA would be appropriate. The next Part seeks to answer that question.

II. ERISA ENFORCEMENT OF HIPAA: SHOULD THERE BE A CAUSE OF ACTION?

Out of respect for the different roles of the legislature and judiciary, courts recognize only those statutory causes of action that Congress intended to create.\footnote{See \textit{Alexander v Sandoval}, 532 US 275, 289 (2001) (holding that a statute must evince "congressional intent to create new rights"); \textit{Cannon v University of Chicago}, 441 US 677, 730–31 (1979) (Powell dissenting) ("When Congress chooses not to provide a private civil remedy, federal courts should not assume the legislative role of creating such a remedy.").} The Supreme Court has held that "the fact that a federal statute has been violated and some person harmed does not automatically give rise to a private cause of action in favor of that person"\footnote{\textit{Cannon}}, and that "private rights of action to enforce federal law must be created by Congress."\footnote{\textit{Alexander}} Although ERISA enforcement of HIPAA is arguably more acceptable than an implied cause of action for HIPAA, courts still will not find a cause of action where Congress intended none to exist. Therefore, whether a court recognizes a private cause of action for privacy-rule violations will depend upon Congress’s intent in enacting the two statutes, as manifested in the statutory language and other expressions of intent.

When courts decide whether to infer a private cause of action from a federal statute, their "focal point is Congress' intent in enacting the statute."\footnote{\textit{Sandoval}, 532 US 275, 289 (2001) (holding that a statute must evince "congressional intent to create new rights"); \textit{Cannon}, 441 US 677, 730–31 (1979) (Powell dissenting) ("When Congress chooses not to provide a private civil remedy, federal courts should not assume the legislative role of creating such a remedy.").} This inquiry does not "require evidence that Members of Congress, in enacting the statute, actually had in mind the creation of a private cause of action."\footnote{\textit{Cannon}} Rather, "Congress' intent may appear implicitly in the language or structure of the statute, or in the circumstances of its enactment."\footnote{Id (internal quotation marks and citation omitted).} However, "unless this congressional intent

\begin{flushright}
\textcopyright2005
\end{flushright}
can be inferred from the language of the statute, the statutory structure, or some other source, the essential predicate for implication of a private remedy simply does not exist." In *Thompson v Thompson*, the Supreme Court determined legislative intent by looking to the context, language, and legislative history of the statute. Subsequently, the Court condensed the inquiry, first examining the statutory text for rights-creating language and then exploring the legislative history. This Part first considers Congress's intent as manifested in the statutory language of both HIPAA and ERISA and then examines the practical impact that ERISA-based enforcement would have on HIPAA's regulatory scheme.

A. Determining Congress's Intent

Only one court has considered an independent cause of action for the HIPAA privacy rules, and no court has considered an ERISA-based cause of action for privacy-rule violations. This Part argues that although, as the *University of Colorado Hospital Authority v Denver Publishing Co* court held, there is no manifest congressional intent to create an independent cause of action under HIPAA, Congress did demonstrate an intent to create an ERISA-based cause of action.

---

91 Id (internal quotation marks and citation omitted).
93 Id at 187 (concluding that an investigation into congressional intent behind the Parental Kidnapping Prevention Act revealed no intent to create a private cause of action to determine the validity of competing state custody decisions).
94 *Sandoval*, 532 US at 288 (beginning the investigation into congressional intent with the "text and structure" of the statute itself). See also *Gonzaga University v Doe*, 536 US 273, 284 n 3 (2002) ("Where a statute does not include this sort of explicit 'right or duty-creating language' we rarely impute to Congress an intent to create a private right of action.").
95 *Sandoval*, 532 US at 288 ("In [Thompson], this sort of 'contemporary legal context' simply buttressed a conclusion independently supported by the text of the statute.").
96 Although the Supreme Court has held that "even the most basic general principles of statutory construction must yield to clear contrary evidence of legislative intent," *National Railroad Passenger Corp v National Association of Railroad Passengers*, 414 US 453, 458 (1974), there is no compelling legislative history regarding HIPAA private remedies. See *University of Colorado Hospital Authority v Denver Publishing Co*, 340 F Supp 2d 1142, 1145 (D Colo 2004); *Wright v Combined Insurance Co of America*, 959 F Supp 356, 363 (ND Miss 1997) ("[I]n HIPAA, the undersigned cannot find any 'manifest congressional intent' to create a new federal cause of action."); *Means v Individual Life & Accident Insurance Co*, 963 F Supp 1131, 1135 (MD Ala 1997) ("[T]he court finds no evidence of congressional intent to create a private right of action under HIPAA.").
97 *University of Colorado*, 340 F Supp 2d 1142 (declining to find a private cause of action in HIPAA privacy rules).
1. Rights-creating language.

When determining whether a private cause of action exists, courts look for "rights-creating language" that distinguishes a statute from other merely regulatory laws. "Right[s]-creating language" is language "explicitly confer[ring] a right directly on a class of persons that include[s] the plaintiff in [a] case."

a) Implied cause of action. The University of Colorado court relied on the lack of rights-creating language to dismiss an implied private cause of action under the HIPAA privacy rules. In that case, a hospital filed a complaint under HIPAA to enjoin a newspaper from publishing information obtained during a hospital peer review proceeding. The hospital alleged that some of the information was subject to protection under HIPAA § 1320d-6. The court found that neither § 1320d-6 nor any other section of HIPAA contains any language conferring privacy rights upon any specific class of persons; HIPAA instead focuses on regulating persons with access to individuals' health information. Because the Supreme Court has held that "[s]tatutes that focus on the person regulated rather than the individuals protected create no implication of an intent to confer rights on a particular class of persons," the University of Colorado court found no implied cause of action.

b) ERISA-based cause of action. Unlike an independent cause of action for privacy-rule violations, however, ERISA-based enforcement finds textual support in ERISA § 502(a). ERISA explicitly allows beneficiaries and participants to sue under the terms of the plan. Likewise, HIPAA explicitly makes reference to and regulates ERISA plans with respect to private health information. These two distinctions, combined with the traditional judicial gloss read into § 502(a)(3), make congressional intent to allow ERISA-based private claims seem much more likely than congressional intent to create an independent cause of action under HIPAA.

When interpreting the rights-creating language of ERISA § 502(a)(3), courts recognize that "Congress intended a federal common law of rights and obligations guided by principles of trust law to develop under ERISA." Thus, courts have traditionally interpreted § 502(a)(3)

100 University of Colorado, 340 F Supp 2d at 1142.
101 Id.
102 Id at 1145.
103 Id at 1144, quoting Sandoval, 532 US at 289 (internal quotation marks omitted).
104 Id.
with a certain gloss of federal common law. Courts recognize that "[w]henever Congress enacts complex and comprehensive legislation, such as ERISA, minor gaps in the legislation are unavoidable," and that "[i]t is the judiciary’s role . . . to fill in these gaps." The Supreme Court has interpreted § 502(a)(3)’s protection to be especially broad. For instance, the Supreme Court in Varity Corp v Howe found an implied cause of action for breach of fiduciary duty in the “catchall” provision of § 502(a)(3). The Court found persuasive the fact that plaintiffs would have to proceed under § 502(a)(3) of ERISA or “have no remedy at all.” Subsequent courts have also allowed actions under § 502 where a plaintiff has “no adequate remedy elsewhere in ERISA’s statutory framework.” Because courts interpret § 502(a)(3)’s rights-creating language broadly, the argument for ERISA-based enforcement for the HIPAA privacy rules is much stronger than that for an implied cause of action under HIPAA.

Although Congress did not explicitly address ERISA enforcement in the text of HIPAA, it might have manifested an intent to create such enforcement in the manner in which the two statutes interact. ERISA § 502(a) allows beneficiaries and participants to sue under the terms of the plan, and Congress specifically included references to ERISA plans in HIPAA’s compliance provisions. Likewise, the privacy rules, as enacted by the Secretary of HHS, specifically require the amendment of “plan documents of the group health plan" and require some plans to provide privacy notices. Although Congress did not enact the specific rules, it gave free reign to the Secretary to do so and could have expected the rule to impact other related regulatory schemes, such as ERISA.

106 For instance, courts have recognized a cause of action for breach of fiduciary duty, as discussed in Part III.C. Jamail, Inc v Carpenters District Council of Houston Pension & Welfare Trusts, 954 F2d 299, 303 (5th Cir 1992).
109 Id at 515. 110 See, for example, Jones v American General Life and Accident Insurance Co, 370 F3d 1065, 1074 (11th Cir 2004).
112 45 CFR § 164.504(f)(2).
113 See id § 164.520(a)(2)(i). Self-insured plans were required to provide these notices to all participants by the compliance date. See id § 164.520(c)(2)(i)(A). New enrollees must be given a copy of the notice upon enrollment and a reminder every three years that the notice is available upon request. See id § 164.520(c)(1).
When Congress passes a law, it is “always appropriate to assume that our elected representatives, like other citizens, know the law” and legislate with full knowledge of the potential effects that an old statute might have on a new one. Courts can, therefore, assume that Congress was aware of the liberal interpretation of ERISA § 502(a)(3) when it passed HIPAA. To the extent that Congress showed awareness of HIPAA’s effects on ERISA plans, and even went so far as to exclude some plans but not others from HIPAA’s requirements, it arguably intended to create an enforcement right for the privacy rules through ERISA’s statutory scheme.

2. Explicit public enforcement provisions.

In addition to rights-creating language, courts also place great weight on whether there is a preexisting public enforcement scheme. Although it is true that a statute providing for a criminal penalty “does not necessarily preclude the implication of a private cause of action for damages,” courts are reluctant to recognize additional remedies where a statute expressly provides one.

In University of Colorado, the district court noted that the presence of a specific civil and criminal enforcement scheme for HIPAA weighed heavily against an implied private cause of action for HIPAA privacy-rule violations. Likewise, when examining a potential cause of action under ERISA § 502(a)(3), the Supreme Court noted that “where Congress elsewhere provided adequate relief for a beneficiary’s injury, there will likely be no need for further equitable relief.”

However, at least one court has opined that the public enforcement provisions of the privacy rules are not the only enforcement mechanism available for those rules. Specifically, in Law v Zucker- man, the court was willing to enforce the privacy rules through the discovery rules of the Federal Rules of Civil Procedure.

\[\text{\footnotesize 115 Cannon, 441 US at 696–97 (holding that awareness of prior judicial interpretation of laws reflects their intent with respect to newly created laws).}\]
\[\text{\footnotesize 116 See 45 CFR § 160.102, excluding those plans that are self-insured plans, are administered by a sole employer, and have fewer than fifty participants.}\]
\[\text{\footnotesize 117 Cort v Ash, 422 US 66, 79 (1975).}\]
\[\text{\footnotesize 118 See Transamerica Mortgage Advisors (TAMA), Inc v Lewis, 444 US 11, 19 (1979). ("[I]t is an elemental canon of statutory construction that where a statute expressly provides a particular remedy or remedies, a court must be chary of reading others into it.").}\]
\[\text{\footnotesize 119 See 340 F Supp 2d at 1144–45.}\]
\[\text{\footnotesize 120 Varity Corp, 516 US at 515.}\]
\[\text{\footnotesize 121 307 F Supp 2d 705 (SD Md 2004).}\]
\[\text{\footnotesize 122 Id at 712 (concluding that since HIPAA does not provide guidance on “how a court should treat . . . a violation during discovery or at trial, the type of remedy to be applied is within the discretion of the Court under [FRCP] 37").}\]
The defendant's attorney in *Law* violated the privacy rules by discussing the plaintiff's health information with her doctor without her permission.\(^{123}\) Although the court ultimately found that limiting subsequent communications between the opposing attorney and the treating physician was unwarranted because of the opposing attorney's good-faith reliance on a state health-privacy statute, it held that the information was obtained in violation of the HIPAA privacy rules and suggested that the information could be held inadmissible at trial.\(^{124}\)

The court recognized that HIPAA has its own enforcement mechanism, but it pointed out that HIPAA does not dictate how a court should treat such a violation during discovery or at trial. Because HIPAA directly regulates discovery but does not provide a specific remedy for discovery abuse, the *Law* court felt free to supplement HIPAA's statutory enforcement provisions under the discovery rules. Following this reasoning, because HIPAA directly regulates ERISA plans without providing a specific remedy for ERISA employment-related violations,\(^ {125}\) a court could find that ERISA's enforcement mechanisms, not HIPAA's, apply to such violations.

In sum, although the legislative history contains no explicit statement of congressional intent to create an ERISA cause of action for violations of the HIPAA privacy rules, Congress created the statutes to interact with each other in such a way as to imply its intent to allow for ERISA enforcement.

B. Impact of ERISA Enforcement on HIPAA's Enforcement Scheme

This Part argues that, like the procedural enforcement of *Law*, ERISA-based enforcement of the HIPAA privacy rules would fully effectuate the purpose of HIPAA without undermining either public enforcement of HIPAA or the ERISA regulatory system. ERISA-based enforcement would be available only in relation to employee benefit plans and, because of the limited remedies available, would likely be used only when state-law claims are preempted.

1. HIPAA in the employment context.

Rules restricting employers' access to employees' health information are essential because ERISA, for the first time, gave employers

\(^{123}\) Id at 707.
\(^ {124}\) Id at 712-13.
\(^ {125}\) See Part I.A.1 for a discussion of HIPAA regulation of ERISA plan usage of health information.
broad access to such information. Congress, in passing HIPAA, recognized that health information had become more vulnerable with the increasing use of electronic storage, which is especially susceptible to unauthorized access. This trend is especially problematic in the employment context: the danger is that employers will make employment decisions based upon private employee health information. Adequate protection for the privacy of health information is important because without it, employees may not confide in their doctors for fear of adverse employment consequences. Allowing ERISA-based enforcement of the privacy rules would strengthen HIPAA’s prohibition on unauthorized employer access without interfering with HIPAA’s general enforcement scheme.

2. Safeguards to overenforcement.

ERISA’s remedies are limited such that a § 502(a)(3) suit would be a plaintiff’s last resort. ERISA § 502(a)(3) authorizes only “appropriate” equitable relief, and the Supreme Court has suggested that “courts, in fashioning ‘appropriate’ equitable relief, will keep in mind the ‘special nature and purpose of employee benefit plans,’ and will respect the ‘policy choices reflected in the inclusion of certain remedies and the exclusion of others.’”

Likewise, whether a court would accept a § 502(a)(3) request for relief for privacy-rule violations would depend on whether it determined that “Congress had elsewhere provided adequate relief for [the] beneficiary’s injury.” Courts could decide on a case-by-case basis


127 See 142 Cong Rec H 9793 (Aug 1, 1996). Representative DeFazio from Oregon said:

In addition, I am very concerned about a provision in the conference report that threaten[s] the continued privacy of our medical records. As Americans we cherish our fundamental right to privacy. Over the past few decades we have seen this right chipped away by technological advances we could never [have] foreseen. We have all seen how legislation ensuring the continued right to privacy has not kept up with these advances. This conference report strikes another blow at our privacy by requiring administrative simplification of medical records without providing adequate protections.


129 See Winn, 33 Rutgers L J at 633 (cited in note 126).


131 Id at 515.
whether HIPAA's enforcement scheme provided adequate relief for a particular plaintiff. Or courts could decide, as the Law court seemed to find, that the civil and criminal penalties authorized under HIPAA are insufficient to enforce the privacy rules in the employment setting.

ERISA-based enforcement would supplement HIPAA's regulatory scheme in the employment context in much the same way the discovery rules supplemented HIPAA in the litigation context. Because of the "regulatory vacuum"\footnote{132 Davila, 124 S Ct at 2503 (Ginsburg concurring).} from possible ERISA preemption and the unique nature of health information in the workplace, ERISA-based enforcement of the privacy rules is consistent with both the "gap-filling"\footnote{133 Susan C. Davis, Bird v. Shearson Lehman/American Express, Inc.: Upholding Compulsory Arbitration of ERISA Claims Properly Treats All Investors Equally, 75 Minn L Rev 123, 151 (1990).} common law interpretation of ERISA, and HIPAA's overall enforcement scheme.

III. ENFORCING HIPAA THROUGH ERISA STATUTORY SUITS

Although courts have yet to consider a cause of action for violations of HIPAA's privacy rules under ERISA § 502(a)(3)'s equitable enforcement of terms of the plan, this Comment contends that such a cause of action would be legally sound.\footnote{134 In passing, some practitioners have flagged this cause of action as a possibility, without providing subsequent analysis. See, for example, Samuel M. Brock III, Angela F. Hill, and Grant P.H. Shuman, Health Related Information and Employment Decisions: Is Your ERISA Plan Subject to Privacy Rights Under HIPAA?, 24 Energy & Mineral L Inst ch 1 at 28 (2004):

"Violations" of HIPAA involving sponsors of group health plans that are covered by HIPAA ... may be subject to a suit under ERISA and ERISA's full panoply of remedies. HIPAA requires that the plan documents of group health plans be amended to include the protections of the Privacy Rules. Thus, plan participants may bring claims for breach of fiduciary duty, or claims to enforce plan provisions or enjoin plan violations, for what, essentially, are violations of HIPAA's Privacy Rules. See also Diane Kutzko, et al, HIPAA in Real Time: Practical Implications of the Federal Privacy Rule, 51 Drake L Rev 403, 450 (2003). These articles focused on only the amendments required under 45 CFR § 164.504(f)(1)-(2), not the privacy notices required under 45 CFR § 160.501.} This Part argues that privacy-rule plaintiffs may be able to enforce the rules as "terms of the plan" or through breach of fiduciary duty claims. Part III.A discusses statutory remedies generally, including proper plaintiffs and defendants and the remedies available under § 502(a)(3). Part III.B argues that HIPAA plaintiffs can sue under the "terms of the plan" either using the amendments to the plan regarding disclosures to a plan sponsor or, more broadly, the privacy notice. Part III.C compares a § 502(a)(3) suit under the terms of the plan with a suit under the same provision for breach of fiduciary duty.
A. Statutory Remedies Generally

ERISA provides for private remedies mainly through § 502(a)(1)(B) and its equitable companion, § 502(a)(3). These two provisions give participants and beneficiaries a cause of action to recover benefits due under the terms of the plan, to enforce rights under the terms of the plan, and to clarify rights to any future benefits under the terms of the plan. Although courts have yet to use ERISA to enforce HIPAA's privacy rules, connecting the dots between ERISA and HIPAA suggests that most violations of HIPAA privacy rules are actionable under the “catchall” provisions of the equitable § 502(a)(3). ERISA § 502 states, in pertinent part:

(a) Persons empowered to bring a civil action. A civil action may be brought ... (3) by a participant, beneficiary, or fiduciary (A) to enjoin any act or practice which violates any provision of this subchapter or the terms of the plan, or (B) to obtain other appropriate equitable relief (i) to redress such violations or (ii) to enforce any provisions of this title or the terms of the plan.

ERISA § 502(a)(3) suits are not limited to suits under the terms of the plan but also include suits for breach of fiduciary duty.

The rest of this Part will discuss proper plaintiffs, defendants, and remedies. It will argue that because proper plaintiffs and remedies are limited, ERISA enforcement of health privacy rules will likely be limited to employment situations preempted by ERISA instead of being used as a general substitute for state privacy law claims. However, because ERISA plaintiffs can sue a broad range of defendants, ERISA-based enforcement will have more bite than the current HIPAA complaint process.

1. Proper plaintiffs and defendants.

Proper plaintiffs under § 502(a) are participants, beneficiaries, or fiduciaries of the plan, or the Secretary of Labor. The general rule

---

135 For a list of examples of 29 USC § 1132(a)(1)(B) litigation, see Zanglein and Stabile, ERISA Litigation at 73-76 (cited in note 64).

136 29 USC § 1132(a)(3).

137 See Varity Corp., 516 US at 512 (interpreting § 502(a)(3) as providing appropriate equitable relief for injuries caused by violations that § 502 does not address elsewhere, including breach of fiduciary duty). See also Devlin v Empire Blue Cross & Blue Shield, 274 F.3d 76, 89 (2d Cir 2001) (“The Supreme Court held that such claims alleging breach of fiduciary duty could be brought by individual plaintiffs.”); Watson v Deaconess Waltham Hospital, 141 F Supp 2d 145, 150 (D Mass 2001) (“The Supreme Court has interpreted ERISA § 502(a)(3) ... to permit an individual to sue directly for a breach of fiduciary duty, as long as she seeks equitable relief.”).
is that nonenumerated parties do not have standing to sue,\(^\text{138}\) and employers usually are excluded.\(^\text{132}\) Additionally, although courts differ on whether plaintiffs with derivative standing\(^\text{140}\) may sue under ERISA § 502(a), in most circuits derivative standing is at least a colorable claim under which assignees may be able to sue to uphold terms of the plan.\(^\text{142}\) If proper plaintiffs have brought the action under § 502(a), the proper venue is a federal court notwithstanding the amount in controversy or the citizenship of the parties.\(^\text{145}\)

More important for a privacy-rule plaintiff is the broad range of potential defendants. Courts have held that a proper plaintiff can bring suit in equity under § 502(a)(3) against third parties "where necessary to redress a violation of the terms of the Plan or to enforce the Plan."\(^\text{131}\) If proper plaintiffs have brought the action under § 502(a), the proper venue is a federal court notwithstanding the amount in controversy or the citizenship of the parties.\(^\text{145}\)

For a complete listing by area of law, see Zanglein and Stabile, *ERISA Litigation* at 113 (cited in note 64).

---

\(^{138}\) Participants are defined as "any employee or former employee of an employer ... who is or may become eligible to receive a benefit of any type from an employee benefit plan which covers employees of such employer." 29 USC § 1002(7).

\(^{139}\) A beneficiary is defined as "a person designated by a participant, or by the terms of an employee benefit plan, who is or may become entitled to a benefit thereunder." Id § 1002(8).

\(^{140}\) Fiduciaries are generally designated as such in the plan documents and are individuals who "have authority to control and manage the operation and administration of [a] plan." Id § 1102(a)(1). For the statutory definition of fiduciaries, see id § 1002(21).

\(^{141}\) For a complete listing by area of law, see Zanglein and Stabile, *ERISA Litigation* at 113 (cited in note 64).

\(^{142}\) See *Healthtek Solutions, Inc v Fortis Benefits Insurance Co*, 274 F Supp 2d 767, 775 (ED Va 2003).

\(^{143}\) An example of derivative standing would be a suit for benefits by a valid assignee. Assignees are those who get their rights assigned to them by an enumerated party (for example, a participant, beneficiary, etc.). Most courts hold that the assignment must be valid in order to sue under the terms of the plan. Zanglein and Stabile, *ERISA Litigation* at 120 (cited in note 64).

\(^{144}\) For a list, by circuit, of examples of derivative ERISA § 502 litigation, see id at 167–68.

\(^{145}\) 29 USC § 1132(e)(1); 29 USC § 1132(f).

\(^{146}\) *Central States, Southeast and Southwest Areas Health and Welfare Fund v Comprehensive Care Corp*, 864 F Supp 831, 833 (ND Ill 1994), discussing *Blue Cross and Blue Shield v Weitz*, 913 F2d 1544 (11th Cir 1990). See also *Milwaukee Carpenter's District Council Health Fund v Philip Morris, Inc*, 70 F Supp 2d 888, 897 (ED Wis 1999) ("[ERISA § 502(a)(3)] is not by its terms limited to suits by fiduciaries against plan participants or beneficiaries, but extends to suits against third parties as well.").

\(^{147}\) See *Great-West Life & Annuity Insurance Co v Knudson*, 534 US 204, 210 (2002) (noting that the proper relief under § 502(a)(3) is limited to those forms of relief that were typically available in equity).

\(^{148}\) See *Harris Trust and Savings Bank v Salomon Smith Barney, Inc*, 530 US 238, 246–47 (2000) (noting that 29 USC § 1132(a)(3) "admits of no limit ... on the universe of possible defendants. Indeed [it] makes no mention at all of which parties may be proper defendants").
2. Equitable relief.

Equitable relief is the proper type of relief for privacy-rule plaintiffs suing under § 502(a)(3). The Supreme Court stated in Great-West Life & Annuity Insurance Co v Knudson that "equitable relief in § 502(a)(3) must refer to those categories of relief that were typically available in equity." In a prior decision, the Court held that restitution is "a remedy traditionally viewed as 'equitable,'" and other courts have recognized that employment reinstatement is an equitable remedy. In Schwartz v Gregori, for instance, the Sixth Circuit determined that the plaintiff had been discharged from her employment in retaliation for exercising her rights under ERISA and was entitled to either reinstatement or front pay under § 502(a)(3).

B. Suits Under the Terms of the Plan

ERISA § 502(a)(3) allows proper plaintiffs to sue to enforce their rights under the terms of the plan. Any changes to ERISA plan documents could potentially be considered changes to the "terms of the plan" under § 502(a)(3). HIPAA requires the production or amendment of ERISA plan documents in two ways. First, it requires plan administrators to amend plan documents in order to prevent misuse of health information by plan sponsors. Second, it requires self-insured group health plans and plans that create or maintain personal health information to provide privacy notices detailing the uses and disclosures of protected health information. This Part will discuss in turn each of these HIPAA documents as a potential basis for suit. This Part argues that of the two, the privacy notice is much broader in scope, applying not only to transactions by the plan sponsor but potentially to all transactions, uses, and disclosures of an individual's health information. If a court were to interpret these HIPAA docu-

---

149 See 29 USC § 1132(a)(3) (providing that plaintiffs suing under the terms of the plan may obtain "other appropriate equitable relief").
150 534 US 204 (2002).
151 Id at 210 (internal quotation marks omitted).
152 Mertens, 508 US at 255.
153 See, for example, Schwartz v Gregori, 45 F3d 1017, 1023 (6th Cir 1995).
154 45 F3d 1017 (6th Cir 1995).
155 The plaintiff sued to enforce her rights as set forth in 29 USC § 1140: "It shall be unlawful for any person to discharge, fine, suspend, expel, discipline, or discriminate against a participant or beneficiary for exercising any right to which he is entitled under the provisions of an employee benefit plan." 45 F3d at 1020.
156 Schwartz, 45 F3d at 1023.
157 See 45 CFR § 164.504(f)(1)–(2).
158 See id § 164.520(a) (covering self-insured plans or plans that produce or maintain private health information).
ments and amendments as embodying "terms of the plan," a violation of those terms would be actionable under ERISA § 502(a)(3).159

1. Plan amendments as terms of the plan.

Because HIPAA requires amendments to ERISA plan documents to restrict disclosures to plan sponsors,160 plaintiffs should be able to enforce those restrictions/amendments as "terms of the plan" under § 502(a)(3). Plan sponsors are required to establish and maintain a plan in accordance with a written document,161 which courts have accepted as containing terms of the plan.162 Amendments to the plan, if valid,163 represent enforceable terms of the plan.164 As the Supreme Court held in Curtiss-Wright Corp v Schoonejongen,165 "Employers or other plan sponsors are generally free under ERISA, for any reason at any time, to adopt, modify, or terminate welfare plans."166 Amendments to the health plan made pursuant to the privacy rules and restricting access to plan sponsors should,167 if properly made, likewise be considered terms of the plan, violations of which are actionable under § 502(a)(3).

2. Privacy notices as terms of the plan.

The second set of documents—privacy notices—provides a broader series of claims, because privacy notices cover disclosures to all third parties, not just plan sponsors. Although some ERISA case law has held that similarly representative documents embody terms of the plan under § 502(a), other courts have been reluctant to find "terms" anywhere outside of the standard plan documents.

a) The split over outside sources. Courts are reluctant to recognize insufficiently formal modifications to an ERISA plan, because ERISA imposes particular requirements upon covered entities for

159 See 29 USC § 1132(a)(3).
160 See 45 CFR § 164.504(f)(1).
161 See 29 USC § 1102.
162 See Moore v Metropolitan Life Insurance Co, 856 F2d 488, 492 (2d Cir 1988) ("Congress intended that plan documents and the [summary plan descriptions] exclusively govern an employer's obligations under ERISA plans.").
163 See, for example, Curtiss-Wright Corp v Schoonejongen, 514 US 73, 78 (1995) (reasoning that a § 402(b)(3) [29 USC § 1102(b)(3)] analysis of the validity of an amendment requires that the plan must set forth who is authorized to amend the plan and how amendments are to be effectuated).
164 See Ross v Rail Car America Group Disability Income Plan, 285 F3d 735, 741–43 (8th Cir 2002) (reasoning that since plan amendments were properly enacted, terms of the plan come from those amendments).
166 Id at 78.
167 See 45 CFR § 164.504(f)(1).
adopting and amending a written plan. The purpose of the required formalities is twofold: to ensure that "proposed plan amendments, which are fairly serious events, are recognized as such and given the special consideration they deserve," and to allow administrators to distinguish "the bona fide amendments from those that are not." Because privacy notices, unlike HIPAA plan amendments, do not necessarily add to or change actual plan documents, whether or not they constitute terms of the plan depends upon their perceived formality and representativeness.

Probably the most widely recognized outside source of plan terms is the "summary plan description." Many courts enforce summary plan descriptions even over conflicting terms in actual plan documents. Although some courts seem to place great weight on the fact that summary plan descriptions are required by § 102 of ERISA, other courts have accepted documents other than summary plan descriptions as containing terms of the plan, so long as those documents are similarly representative. In Brines v XTRA Corp, the Seventh Circuit noted that while informal modifications of ERISA plans are not permitted, prior cases have recognized plan modifications even in the absence of formal documentation. Additionally, since employers often have different plans covering different benefits, informal documentation could arguably constitute a separate and enforceable plan, so long as it does not contradict the written plan.

---

168 See Winterrowd v American General Annuity Insurance Co, 321 F3d 933, 937–38 (9th Cir 2003) (explaining that the purpose of § 402's amendment procedures is to prohibit plan modifications that are too informal).
169 Curtiss-Wright Corp, 514 US at 82.
170 Id. See HR Rep No 1280, 93d Cong, 2d Sess (1974), reprinted at 1974 USCCAN 5077–58 ("A written plan is to be required in order that every employee may, on examining the plan documents, determine exactly what his rights and obligations are under the plan.")
171 Summary plan descriptions are defined in the statute as "sufficiently accurate and comprehensive to reasonably apprise such participants and beneficiaries of their rights and obligations under the plan." 29 USC § 1022(a).
172 Specifically, the Second, Fifth, Sixth, Seventh, Eighth, Tenth, and Eleventh Circuits have all held that the summary plan description trumps other plan documents. For a more complete listing by circuit, see Zanglein and Stabile, ERISA Litigation at 467 n 69 (cited in note 64).
173 See, for example, Burstein v Retirement Account Plan for Employees of Allegheny Health Educ & Research Found, 334 F3d 365, 379–80 (3d Cir 2003) (finding that summary plan descriptions are required by § 102 (29 USC § 1022) and are meant to be "accurate" and "sufficiently comprehensive to reasonably apprise plan participants of their rights and obligations under the plan").
174 See, for example, Kochendorfer v Rockdale Sash and Trim Co, Inc Profit Sharing Plan, 653 F Supp 612, 614–16 (ND Ill 1987) (accepting a record-keeping booklet given to a participant in a profit-sharing plan as a summary plan description).
175 304 F 3d 699 (7th Cir 2002).
176 See id at 701–02.
177 See id.
Not all courts accept summary plan descriptions or other less official documents as terms of the plan, however. In *O'Brien v Sperry Univac*, the court acknowledged that "the statute's definition of 'plan' is not limited to a single document," but ultimately rejected the plaintiff's argument that the summary plan description contained "terms of the plan." Likewise, another court held that outside documents cannot invalidate actual portions of the plan. In *Moore v Metropolitan Life Insurance Co*, the Second Circuit explained the policy reasons for limiting sources of terms of the plan:

Congress intended that plan documents and [summary plan documents] exclusively govern an employer's obligations under ERISA plans. . . . Were all communications between an employer and plan beneficiaries to be considered . . . as establishing the terms of a welfare plan, the plan documents . . . would establish merely a floor for an employer's future obligations. Predictability as to the extent of future obligations would be lost, and, consequently, substantial disincentives for even offering such plans would be created.

Another court held that the crucial issue is to identify "which of the plethora of papers proffered by parties constitute 'official plan documents.'" In reaching its conclusion, the court noted the inherent difficulty in determining what constitutes a sufficiently official plan document containing terms of the plan:

Both sides agree on the obvious ends of the spectrum: Each version of the Plan itself is an official plan document, while a number of letters and interoffice memoranda are not. However, the parties seem to part company over which of the many booklets distributed to employees constitute official plan documents.

Whether privacy notices are closer to one end or the other of the spectrum depends, then, upon judicial determinations of their formality and representativeness.

*b) Privacy notices as outside sources.* Privacy notices play a role similar to that of summary plan descriptions: they explain the rights and duties of parties with regards to the plan. Covered ERISA plans must provide the notices to all participants. Privacy notices, like sum-

---

178 458 F Supp 1179 (D DC 1978).
179 Id at 1180.
181 856 F2d 488 (2d Cir 1988).
182 Id at 492.
184 Id (internal citations omitted).
mary plan descriptions, are subject to highly formalized regulations governing content and means of dissemination. As explained in Part I.A, privacy notices must be written in plain language, include an example of a permitted disclosure, and detail all disclosures that can be made without the participant’s consent.

The requirements for privacy notices suggest that such notices, like summary plan descriptions, represent the rights and obligations of parties regarding health information. For instance, the following statement must feature prominently in every privacy notice: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.” Likewise, the language of privacy notices appears to represent rights and duties; for instance, a privacy notice might include a section stating that:

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission, unless those uses can be reasonably inferred from the intended uses above. If you have provided us with your permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

Privacy notices clearly seem to fulfill the first policy behind requiring formal amendments: flagging for beneficiaries important changes regarding changes to their rights under the plan.

In addition to bringing important plan changes to the attention of beneficiaries, requiring formal plan amendments also promotes administrative efficiency by helping administrators to distinguish between bogus and bona fide plan modifications. Some courts have

185 Compare 29 USC § 1022, with 45 CFR § 164.520.
186 45 CFR § 164.520(b)(1)(i).
188 See Curtiss-Wright, 514 US at 82. During debates for the Bipartisan Patient Protection Act, S 872, 107th Cong, 1st Sess (May 14, 2001), which passed the Senate in 2001 but failed to pass in the House of Representatives, see States News Service, Sen. Boxer Introduces Patients' Bill of Rights (Feb 17, 2004), at least one member of Congress expressed concern that giving patients a private cause of action against HMOs and ERISA self-insured employers would prompt small businesses to drop their insurance coverage rather than risk being sued. 147 Cong
expressed concern that holding plan sponsors to terms found outside of the standard plan documents will lead to unpredictability and a disincentive to provide employee benefit plans. Obviously, a cause of action that so threatens HIPAA’s stated goal—to improve access to healthcare—is antithetical to the statute’s purpose. Allowing suits for privacy-rule violations could conceivably open the floodgates of litigation and uncertainty, thereby driving up the costs of healthcare and making employer-provided healthcare prohibitively expensive.

Use of privacy notices to determine terms of the plan may not, however, actually implicate the legitimate concerns raised by other non-plan documents. For instance, privacy notices are standard statutory requirements, and thus their use as sources of terms of the plan is unlikely to create uncertainty. On the contrary, the particular language and formality of privacy notices may already induce plan participants to rely upon them as binding terms of the plan. If so, courts may foster unpredictability by not including their provisions as “terms of the plan.”

Similarly, enforcement of HIPAA through ERISA does not give rise to the difficulties that might inhere in an independent cause of action for privacy violations under HIPAA itself. ERISA’s statutory enforcement mechanism would provide broad but not limitless protection for privacy-rule plaintiffs. Plaintiffs could bring suit against third parties where “necessary to redress a violation of the terms of the Plan or to enforce the Plan.” The privacy rules do not cover all protected health information usage, however, but only usage by specified covered entities, which excludes most small businesses that self-insure. Additionally, § 502 specifies that only a “participant, beneficiary, or fiduciary” of an ERISA health plan may bring a private enforcement suit.

Rec § 6837 (June 25, 2001) (Senator Gregg) (“For the 56 million people who are covered by self-insured plans...the fact is, you can sue the employer. ... [A] lot of employers are going to drop their insurance so the people who have insurance today will not have it tomorrow.”). 189 See, for example, Sprague v General Motors Corp, 133 F3d 388, 402 (6th Cir 1998) (“The writing requirement ensures that every employee may, on examining the plan documents, determine exactly what his rights and obligations are under the plan. ... [T]he requirement lends predictability and certainty to employee benefit plans. [This] serves the interests of both employers and employees.”); Gable v Sweetheart Cup Co, 35 F3d 851, 857 (4th Cir 1994) (“Were we to hold that other communications could nullify this express written term, plan documents would no longer serve to ensure predictability as to employers’ future liabilities, and consequently, substantial disincentives for even offering such plans would be created.”) (internal quotation marks omitted); Moore, 856 F2d at 492 (concluding that ERISA plans are not “subject to amendment as a result of informal communications”).

189 Central States, Southeast and Southwest Areas Health and Welfare Fund v Comprehensive Care Corp, 864 F Supp 831, 833 (ND Ill 1994).

190 See 45 CFR § 164.500.

191 Covered entities essentially include all ERISA plans except those self-insured plans that are administered by a sole employer and have fewer than fifty participants. See 45 CFR § 160.102.

192 29 USC § 1132(a)(3).
Nor do HIPAA's required amendments and privacy notices include all possible privacy-rule rights or violations. The amendments to plan documents relate only to how and when an employer can access employee health information. Likewise, privacy notices restrict use and disclosure of health information only with respect to the entity giving notice and the individual receiving notice.\(^{194}\) Moreover, additional relief would be limited to equitable relief; monetary relief would be available only under very limited circumstances.\(^{195}\) Because ERISA enforcement of the privacy rules would be restricted, there is no reason to believe that such enforcement would result in disincentives to provide employee benefit plans.

C. Suit for Breach of Fiduciary Duty

Another possible suit under ERISA \(\S\) 502(a)(3) is a suit for breach of fiduciary duty,\(^{196}\) which would not require a finding that privacy notices constitute terms of the plan. The claim for breach of fiduciary duty is a hybrid of a relatively new statutory cause of action and its former common-law incarnation. Although the Supreme Court has held that suits for breach of fiduciary duty fall under the "catchall" provision of \(\S\) 502(a)(3), the lower courts have narrowly construed that holding as applying only when a proper plaintiff has "no adequate remedy elsewhere in ERISA's statutory framework."\(^{197}\) Additionally, courts continue to rely on their common law precedents to define what constitutes a breach of fiduciary duty under ERISA.\(^{198}\) A breach of fiduciary duty claim requires that a plaintiff prove more elements than does a suit under the "terms of the plan."\(^{199}\)

This Part will first discuss what a breach of fiduciary suit will look like when plaintiffs rely on the privacy notice. Since not all ERISA plans must produce privacy notices, this Part will next examine whether a plaintiff can state a valid cause of action without relying on a privacy

\(^{194}\) See 45 CFR \(\S\) 164.520(b)(ii).

\(^{195}\) Great-West, 534 US at 209, 213 (acknowledging that a sum of money might constitute "appropriate equitable relief" in very limited circumstances, "where money or property identified as belonging in good conscience to the plaintiff could clearly be traced to particular funds or property in the defendant's possession," but holding that money damages do not typically qualify as equitable relief).

\(^{196}\) See Varity Corp, 516 US at 507-15 (interpreting \(\S\) 502(a)(3) as providing appropriate equitable relief for injuries caused by violations that \(\S\) 502 does not address elsewhere, including breach of fiduciary duty).

\(^{197}\) See Jones v American General Life and Accident Insurance Co, 370 F3d 1065, 1074 (11th Cir 2004).

\(^{198}\) See, for example, id at 1072-74 (applying the common law of misrepresentation).

\(^{199}\) See text accompanying note 201.
notice. Lastly, this Part considers whether a breach of fiduciary duty claim exists whenever a fiduciary violates HIPAA regulations.

1. Relying on a privacy notice.

Many circuits have held that ERISA creates a federal cause of action for breach of fiduciary duty for providing inaccurate information. If a plan has established and maintained a privacy notice and a fiduciary refuses to honor those rights manifested in the notice, that fiduciary may be liable for breach of fiduciary duty. Most courts require that plaintiffs in such cases show: “(1) that the defendant was acting in a fiduciary capacity when it made the challenged representations; (2) that these constituted material misrepresentations; and (3) that plaintiffs relied on those misrepresentations to their detriment.”

Although *Harris Trust and Savings Bank v Salomon Smith Barney, Inc* permits suits against certain nonfiduciaries for breach of fiduciary duty, courts continue to require that defendants were acting as fiduciaries when the misrepresentations were made. Even a defendant who qualifies as a fiduciary under common law is an ERISA fiduciary “only when fulfilling certain defined functions, including the exercise of discretionary authority or control over plan management or administration.” The decision to comply with HIPAA regulations might be considered such an exercise of control over plan administration.

The requirement of reasonable and detrimental reliance is a stringent one. The Fourth Circuit requires, for instance, that the detrimental reliance “take the form of a definite and identifiable action” and has held that, “[s]pecifically, an estoppel arises when one person makes a definite misrepresentation of fact to another person having

---

200 See, for example, *Drennan v General Motors Corp*, 977 F2d 246, 251 (6th Cir 1992) (“Misleading communications to plan participants regarding plan administration (for example, eligibility under a plan, the extent of benefits under a plan) will support a claim for a breach of fiduciary duty.”) (internal quotation marks and citation omitted).

201 *James v Pirelli Armstrong Tire Corp*, 305 F3d 439, 449 (6th Cir 2002) (holding that an employer breached its fiduciary duty by providing materially misleading or inaccurate information to employees about its pension/severance plan).


203 See id at 246–47.

204 See *Daniels v Thomas & Betts Corp*, 263 F3d 66, 73 (3rd Cir 2001) (stating that a plaintiff must establish “the defendant’s status as an ERISA fiduciary acting as fiduciary” in order to make out one element of a breach of fiduciary duty claim); *McMunn v Pirelli Tire, LLC*, 161 F Supp 2d 97, 125 (D Conn 2001). Acting like a fiduciary means having “authority to control and manage the operation and administration of [a] plan.” See 29 USC § 1102(a)(1).


reason to believe that the other will rely upon it and the other in rea-
sonable reliance does an act.\textsuperscript{207}

Although such reliance theoretically could consist merely of con-
tinuing to participate in the plan, the First Circuit has required that
the plaintiff rely “in such a manner as to change his position for the
worse.”\textsuperscript{208} Since the privacy rules have been in effect for only a short
time, the great majority of ERISA participants have presumably en-
tered into their employment and plan participation without relying on
the rights and protections that the privacy rules afford. However, use
of certain benefits, such as an employee substance abuse program,
could constitute sufficient reliance on the plan’s promise that the em-
ployer would not have access to that health information. Thus, the det-
terimental reliance requirement is demanding but not impossible to meet.

2. No privacy notice.

Even in the absence of a privacy notice, a cause of action for
breach of fiduciary duty for privacy-rule violations may exist under
ERISA \textsuperscript{209} § 409(a). Failure to comply with HIPAA’s requirement that a
privacy notice be issued could constitute a breach of fiduciary duty.
ERISA requires a fiduciary to “discharge his duties with respect to a
plan solely in the interest of the participants and beneficiaries.”\textsuperscript{210} Case
law on the subject is sparse; no court has determined whether a viola-
tion of a federal statute such as HIPAA qualifies as a breach of fiduci-
ary duty, apart from any misrepresentations made. However, misuse of
personal health information may be a breach of the duty to act “solely
in the interest of participants and beneficiaries”\textsuperscript{211} and, thus, a breach
of fiduciary duty.

CONCLUSION

ERISA \textsuperscript{212} § 502(a)(3) should provide a private cause of action to
enforce HIPAA’s privacy rules as terms of the plan or for breach of
fiduciary duty for violations of those rules. Although commentators
and courts have almost uniformly concluded that HIPAA contains no
independent federal private cause of action for privacy-rule violations,
feasible private enforcement mechanisms exist under the enforcement
scheme of its fellow legislation, ERISA.

\textsuperscript{207} Id at 447 (internal quotation marks and citations omitted).
\textsuperscript{208} Law v Ernst & Young, 956 F2d 364, 368 (1st Cir 1992) (internal quotation marks omitted).
\textsuperscript{209} 29 USC § 1109(a)(1).
\textsuperscript{210} Id § 1104(a)(1).
\textsuperscript{211} Id.