Vanderbilt Law Review

Volume 60 | Issue 1 Article 5

1-2007

Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations

Joshua D.W. Collins

Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations

I. INTRODUCTION

"All that may come to my knowledge in the exercise of my profession . . . which ought not to be spread abroad, I will keep secret and will never reveal."

—Hippocratic Oath.[1]

A Midwestern banker, who also served as a member of his county's health board, cross-referenced a health board's list of patients suffering from various diseases with a list of the bank's customers. He then called due the mortgages of anyone suffering from cancer.[2] In Oregon, computer disks containing the medical records of 365,000 patients were stolen from a car. Along with personal medical information, the records also contained the patients' names, addresses, and Social Security numbers.[3] A Maryland school board member's medical records, revealing that he had been treated for depression, were sent to school officials along with an anonymous note that read, "Is this the kind of person we want on the School Board?"[4]

These are just a few of the many recent incidents confirming that breaches of medical privacy occur on a disturbingly regular

---

1. Andrew A. Skolnick, *Opposition to Law Officers Having Unfettered Access to Medical Records*, 279 JAMA 257, 257 (1998).

> The professional codes of nearly every health care profession (for example, the ethics codes for physicians, nurses, dentists and dental hygienists, mental health professionals, social workers, pharmacists, and chiropractors) and the ethical standards of numerous health care professional associations (for example, hospitals and health care executives) all explicitly require respect for the principles of privacy and confidentiality. The codes may refer to privacy or confidentiality as a 'core value' or a 'fundamental tenet' and usually make respect for privacy a central or guiding principle of the health professions.

Charity Scott, *Is Too Much Privacy Bad For Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U.L. REV. 481, 493-94 (2000).

2. Marianne Lavelle, *Health Plan Debate Turning to Privacy; Some Call For Safeguards on Medical Disclosure. Is a Federal Law Necessary?*, NAT'L L. J., May 30, 1994, at A1.

3. Joe Rojas-Burke & Joseph Rose, *365,000 Lose Health Files to Thief*, THE OREGONIAN, Jan. 26, 2006, at A1.

4. Christina A. Samuels, *Allen Makes Diagnosis of Depression Public; Medical Records Mailed Anonymously*, WASH. POST, Aug. 26, 2000, at V1.

basis.[5] The nature of the information contained in medical records and the potentially devastating results of improper disclosures make medical privacy violations abhorrent. Medical records contain highly sensitive information, including intimate details about the patient's illnesses, sexually transmitted diseases, genetic abnormalities, drug and alcohol addictions, and mental or psychological disorders.[6] These records also often include information about the patient's financial status, social behaviors, and personal relationships,[7] as well as identifying information like Social Security numbers.[8] Improper disclosure of such sensitive information may subject patients to social isolation, discrimination by employers, or denial of insurance coverage.[9]

The Health Insurance Portability and Accountability Act ("HIPAA"), adopted by Congress in 1996, aims to protect the security and privacy of health information.[10] The regulations promulgated pursuant to this Act apply to "covered entities," which include (1) health plans, such as health insurance companies, HMOs, Medicare, and Medicaid; (2) health care clearinghouses, such as billing companies and third party administrators; and (3) health care providers, such as hospitals and doctors.[11] These regulations protect patient privacy by restricting disclosure of health information to the "minimum necessary," while also preventing unauthorized use by "downstream users."[12]

While HIPAA imposes a host of obligations on covered entities in an attempt to increase patient privacy, it does not explicitly create any individual rights for patients affected by medical privacy violations. Therefore, a patient who has been seriously harmed as a result of these privacy leaks cannot bring a lawsuit against the responsible party. Instead, a victim's only recourse is to file a

---

5. For more examples of similar medical privacy violations, see Health Privacy Project, Medical Privacy Stories, http://www.healthprivacy.org/usr_doc/Privacy_Violations.pdf.

6. Amy M. Jurevic, *When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail*, 66 UMKC. L. REV. 809, 809-10 (1998).

7. Lawrence O. Gostin et al., *The Nationalization of Health Information Privacy Protections*, 8 CONN. INS. L.J. 283, 284-85 (2002).

8. Jean P. Fisher, *Hacker Hits Duke System; Personal Data, Passwords Taken*, NEWS & OBSERVER (Raleigh, N.C.), June 4, 2005, at D1.

9. *See* Gostin et al., *supra* note 7, at 285 (detailing some of the results of medical privacy violations); Jurevic, *supra* note 6, at 810 (same).

10. 45 C.F.R. §§ 160, 164 (2006). The HIPAA provisions relating specifically to the confidentiality of medical records will hereinafter he referred to as the "Privacy Rule."

11. 45 C.F.R. § 160.103 (2006).

12. *See* 45 C.F.R. § 164.502(e)(1) (stating that a covered entity may only release protected health information to its business associates if it receives satisfactory assurance that the business associate will take the appropriate steps to ensure the confidentiality of the information).

complaint with the Department of Health and Human Services ("HHS").[13] If HHS decides to pursue a victim's complaint, it may impose fines against the responsible covered entity.[14] However, since HIPAA's enactment, HHS has rarely imposed fines or criminal sanctions.[15] Regardless of any enforcement action taken by HHS, the victim will not be compensated for the harm caused by this breach of privacy.

Lack of medical record protection does not just harm those whose privacy is violated; it can have negative effects on the entire healthcare system. Although a majority of Americans are concerned about their medical privacy, many do not understand their rights under HIPAA.[16] As a result, individuals do not have faith in the health care system's ability to protect their medical privacy. Despite the protections provided by HIPAA's Privacy Rule, this mistrust leads one in eight patients to engage in "privacy protective behaviors,"[17] such as providing inaccurate information to doctors or avoiding treatment altogether.[18] Lack of full participation in the health care system not only puts these mistrusting individuals at a significant health risk;[19] it also can be detrimental to the health care system and society as a whole. For example, privacy protective behaviors make "the clinical information used for research, public health initiatives, outcomes analyses, and other studies . . . unreliable."[20] Thus, medical privacy remains a major health care issue because the current protections afforded by the Privacy Rule have not been sufficient to solve this problem.

Unenforced rules are futile. HIPAA created federal rules in order to remedy a perceived problem in the health care industry—the lack of medical privacy. However, if there is no way for health care

13. 45 C.F.R. § 160.306.

14. 42 U.S.C. § 1320d-6(b) (2006).

15. According to one report, HHS had not yet brought a single civil enforcement action under HIPAA as of November, 2005. Joseph Conn, *Ruling Called HIPAA Barrier*, MODERN HEALTHCARE, Nov. 14, 2005, at 16. There has only been one criminal conviction under HIPAA. United States v. Gibson, No. CR04-0374RSM, 2004 WL 2188280 (W.D. Wash. Aug. 19, 2004); Trial Pleading, United States v. Gibson, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. Aug. 19, 2004).

16. A recent survey by the California HealthCare Foundation found that "[d]espite new federal protections, 67 percent of Americans remain concerned about the privacy of their personal health information and are largely unaware of their rights." California HealthCare Foundation, Americans Have Acute Concerns about the Privacy of Personal Health Information (Nov. 9, 2005), http://www.chcf.org/press/view.cfm?itemID=115814.

17. *Id.*

18. Janlori Goldman, *The New Federal Health Privacy Regulations: How Will States Take the Lead?*, 29 J.L. MED. & ETHICS 395, 396 (2001).

19. California HealthCare Foundation, *supra* note 16.

20. Goldman, *supra* note 18, at 396.

consumers to enforce the rules, and no way for them to ensure that HHS enforces the rules, the Act will not achieve its objectives. Health care providers cannot be expected to fully protect patient information without adequate incentives. As former HHS Secretary Donna Shalala stated, "Only if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibilities seriously."[21] Unless patients harmed by the improper disclosure of their private medical records are able to bring actions against the responsible parties, HIPAA's Privacy Rule will remain woefully under-enforced, and Congress's goal of protecting medical privacy will remain frustratingly out of reach.

This Note will explore several potential private rights of action that individuals could bring against entities that improperly disclose patients' medical records in violation of HIPAA's Privacy Rule. Section II will analyze the possibility of bringing a § 1983 claim against an entity that improperly discloses medical records. However, it will argue that the Supreme Court's recent decisions in this area have severely limited the availability of § 1983. As a result, plaintiffs probably cannot use § 1983 to enforce Privacy Rule violations. Section III will discuss the False Claims Act and analyze the opportunity for qui tam plaintiffs to bring an action against the offending party on behalf of the federal government. Though such action may be possible, this Section will show that qui tam enforcement of the Privacy Rule would be contrary to the policies and legal standards set forth by the Supreme Court, and therefore courts should not allow patients to bring these actions. Section IV will advance tort law as a possible solution to this problem and argue that the traditional breach of confidentiality cause of action should be reanalyzed in light of HIPAA standards in order to provide patients with a means of redress for Privacy Rule violations.

II. SECTION 1983

A. Background

42 U.S.C. § 1983 allows plaintiffs to sue parties who deprive them of federally secured rights. It provides:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State . . . subjects, or causes to be subjected, any citizen of the United States or

21. Proposed Rules, Department of Health and Human Services, 64 Fed. Reg. 59,923 (Nov. 3, 1999).

> other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress . . .[22]

Prior to 1980, § 1983 was narrowly construed to prevent private enforcement of civil rights.[23] This barrier to private enforcement was compounded by the Supreme Court's decision to limit implied rights of action dramatically by presuming that no such right existed absent a finding of affirmative legislative intent to the contrary.[24] As a result, the beneficiaries of federal statutes "had a recognized primary right—i.e., a duty owed them by the state—but no remedial right with which to enforce it."[25]

The Supreme Court addressed this problem in *Maine v. Thiboutot*.[26] In *Thiboutot*, the Court faced the issue of whether § 1983 was limited to the enforcement of constitutional rights, civil rights, and equal protection laws, or whether it could be used to enforce state violations of rights conferred by any statute. Making a textual argument, the Court held that the words "and laws" in § 1983 must refer to statutes in order to add independent meaning to the phrase "secured by the Constitution and laws."[27] Therefore, the Court held that § 1983 could be used to enforce rights conferred in any statute.

Since *Thiboutot*, § 1983 has played an important role in the enforcement of private rights by empowering private citizens to bring actions against those who are not in compliance with constitutional or statutory requirements. However, the Court has chipped away at *Thiboutot's* broad interpretation of § 1983, a trend culminating in *Gonzaga University v. Doe*[28] and *City of Rancho Palos Verdes v. Abrams*.[29]

B. Limiting § 1983 Actions

1. *Gonzaga University v. Doe*

In *Gonzaga University v. Doe,* the Supreme Court significantly limited a civil rights plaintiff's ability to bring a private action under

---

22. 42 U.S.C. § 1983 (2006).

23. Sasha Samberg-Champion, *How to Read* Gonzaga*: Laying the Seeds of a Coherent Section 1983 Jurisprudence*, 103 COLUM. L. REV. 1838, 1842-43 (2003).

24. Transamerican Mortgage Advisors, Inc. v. Lewis, 444 U.S. 11, 19-20 (1979); Touche Ross & Co. v. Redington, 442 U.S. 560, 570-71 (1979).

25. Samberg-Champion, *supra* note 23, at 1844.

26. Maine v. Thiboutot, 488 U.S. 1 (1980).

27. *Id.* at 4-5.

28. Gonzaga Univ. v. Doe, 536 U.S. 273 (2002).

29. City of Ranch Palo Verdes v. Abrams, 544 U.S. 113 (2005).

§ 1983. The Court held that the Family Educational Rights and Privacy Act ("FERPA")[30] did not create any individual rights capable of § 1983 enforcement.[31] Doe, a student at Gonzaga University ("Gonzaga"), was denied certification as a Washington schoolteacher when a Gonzaga employee contacted the state agency responsible for teacher certification and, identifying the student by name, informed the agency that the university was investigating him for possible sexual misconduct.[32] Doe brought a § 1983 action against Gonzaga, alleging that it had violated his rights under FERPA by releasing personal information without his consent.[33]

Before ultimately rejecting Doe's claim, the Court noted that its previous decisions in this area were not entirely clear and decided to resolve the ambiguity in its § 1983 jurisprudence by explicitly narrowing the standard for finding rights that are capable of § 1983 enforcement.[34] First, the Court noted that "Section 1983 provides a remedy only for the deprivation of 'rights, privileges, or immunities secured by the Constitution and laws' of the United States. Accordingly, it is *rights*, not the broader or vaguer 'benefits' or 'interests,' that may be enforced under the authority of that section."[35] Thus, the Court emphasized that a "violation of a federal *right*, not merely a violation of federal *law*" is required to establish an action under § 1983.[36] Second, the Court held that only "unambiguously conferred" rights give rise to § 1983 actions, explicitly rejecting the notion that anything less would provide grounds for a § 1983 suit.[37] Whether Congress has conferred a right is a question of congressional intent—an inquiry no different from that required in implied right of

30. FERPA provides that "[n]o funds shall be made available under any application program to any educational agency or institution which has a policy or practice of permitting tbe release of education records (or personally identifiable information contained therein . . .) of students without the written consent of their parents to any individual, agency, or organization." 20 U.S.C. § 1232g(b)(1) (2006). It was enacted pursuant to Congress' spending power, and calls for the withholding of federal funds from educational institutions that fail to adequately protect their students' educational records. *Gonzaga*, 536 U.S. at 278-79.

31. *Id.* at 276.

32. *Id.* at 277.

33. *Id.*

34. *Id.* at 278, 280-86. As one commentator has stated, this intentional decision by the Court to clarify its prior holdings in regards to Section 1983 gives this opinion "importance far beyond its immediate context," and as such is the seminal case in determining whether a Section 1983 action exists under HIPAA. Mark Andrew Ison, *Two Wrongs Don't Make a Right: Medicaid, Section 1983 and the Cost of an Enforceable Right to Health Care*, 56 VAND. L. REV. 1479, 1504 (2003).

35. *Gonzaga*, 536 U.S. at 283 (quoting 42 U.S.C. § 1983 (2002)).

36. *Id.* at 282 (quoting Blessing v. Freestone, 520 U.S. 329, 340 (1997)).

37. *Id.* at 282-83.

action cases.[38] In order for Congress to confer a right on an individual, the statute must be "phrased in terms of the persons benefited" instead of in terms of the party that the law is seeking to regulate.[39] Thus, the Court made it clear that congressional intent determines whether a statute is enforceable by § 1983.

Having established the standard for determining whether a § 1983 claim exists, the Court examined FERPA's text and held that its nondisclosure provisions unquestionably fail to confer enforceable rights.[40] First, the Court noted that FERPA does not focus on the rights of individual students, but instead speaks to the Secretary of Education, directing the Secretary to deny funding to institutions that have policies or practices that violate the statute.[41] Since "[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,' "[42] the Court held that FERPA lacked the rights-creating language that triggers § 1983.[43] Additionally, the Court noted that "FERPA's nondisclosure provisions . . . speak only in terms of institutional policy and practice, not individual instances of disclosure"[44] and that this sort of " 'aggregate' focus" cut strongly against the argument that Congress intended to confer individual rights.[45] Finally, the Court noted that institutions need only substantially comply with FERPA's requirements in order to keep their federal funding.[46] This vague standard, requiring the Secretary of Education to use independent judgment to determine whether institutions have violated this Act, suggests that Congress did not intend to create individually enforceable rights.

It is clear that *Gonzaga* significantly heightened the standard for § 1983 actions, allowing only the clearest and most explicitly conferred rights to be enforced. However, the Court went one step further in *City of Rancho Palos Verdes v. Abrams*.[47]

38. *See id.* at 290 ("[I]f Congress wishes to create new rights enforceable under § 1983, it must do so in clear and unambiguous terms – no less and no more than what is required for Congress to create new rights enforceable under an implied private right of action.").

39. *Id.* at 284 (quoting Cannon v. Univ. of Chi., 441 U.S. 677, 692 n.13 (1979)).

40. *Id.* at 287.

41. *See id.* (quoting 20 U.S.C. §1232g(b)(1) (2002)).

42. *Id.* at 287 (quoting California v. Sierra Club, 451 U.S. 287, 294 (1981)).

43. *Id.*

44. *Id.* at 288.

45. *Id.* (quoting Blessing v. Freestone, 520 U.S. 329, 343 (1997)).

46. *Id.*

47. City of Ranch Palo Verdes v. Abrams, 544 U.S. 113 (2005).

2. *City of Rancho Palos Verdes v. Abrams*

In *City of Rancho Palos Verdes v. Abrams*, the Supreme Court further restricted the use of § 1983. The Court held that a plaintiff could not use § 1983 to enforce certain provisions of the Telecommunications Act ("TCA"), reasoning that the presence of an independent judicial remedy within the statute itself shows that Congress did not intend for it to be enforced through a separate statutory vehicle.[48]

The Court built upon its prior holding in *Gonzaga* by focusing its inquiry solely on whether Congress intended to create a right enforceable under § 1983. The Court did not dispute the fact that the TCA created individually enforceable rights;[49] however, it noted that the existence of such rights does not end the inquiry. Rather, individually enforceable rights create a rebuttable presumption of § 1983 enforcement that may be defeated by demonstrating a lack of congressional intent for such a remedy.[50]

Since the Court found that the TCA provided for a judicial remedy completely independent of § 1983,[51] the central question became whether Congress intended that remedy "to coexist with an alternative remedy available in a § 1983 action."[52] The Court decided that this could not be the case, reasoning that "[t]he provision of an express, private means of redress in the statute itself is ordinarily an indication that Congress did not intend to leave open a more expansive remedy under § 1983."[53] By including a non-§ 1983 judicial remedy, Congress precluded resort to § 1983.[54]

While *Abrams* makes clear that statutes containing a provision for independent judicial remedies cannot be enforced under § 1983, it does not indicate whether statutes providing for administrative remedies, such as those contained in HIPAA, would be barred under the same line of reasoning.

---

48. *Id.* at 120-21.

49. *Id.* at 120.

50. *Id.* (quoting Blessing v. Freestone, 520 U.S. 329, 341 (1997)).

51. *Id.* at 116. The TCA provides that "[a]ny person adversely affected . . . may, within 30 days after such action or failure to act, commence an action in any court of competent jurisdiction." 47 U.S.C. § 332(c)(7)(B)(iii) (2005).

52. *Abrams*, 544 U.S. at 121.

53. *Id.*

54. *Id.* at 127.

C. Using § 1983 to Enforce the Privacy Rule

Plaintiffs seeking to use § 1983 to redress Privacy Rule violations must allege that HIPAA gives them the right to medical privacy and that the defendant deprived them of this right by disclosing their private medical information. However, the Supreme Court's trend toward limiting the applicability of § 1983 makes it doubtful that a plaintiff could successfully use § 1983 to enforce a violation of HIPAA's Privacy Rule. The Privacy Rule ostensibly lacks the explicit rights-creating language that the court required in *Gonzaga*. Additionally, *Abrams* poses a barrier to the use of § 1983 to enforce Privacy Rule violations since the administrative remedies set forth by HIPPA arguably preclude resort to § 1983.

1. *Gonzaga* Precludes Enforcement of the Privacy Rule Through § 1983

While it is not clear exactly how far *Gonzaga* extends, it would nevertheless seem to preclude § 1983 as a potential avenue for the enforcement of HIPAA's Privacy Rule, which "lack[s] the sort of 'rights-creating' language critical to showing the requisite congressional intent to create new rights."[55] The *Gonzaga* Court pointed to Title VI of the Civil Rights Act of 1964 and Title IX of the Education Amendments of 1972 as examples of statutes that create individual rights because they unmistakably focus on the benefited class[56] by stating that that "[n]o person . . . shall . . . be subjected to discrimination . . . ."[57] In contrast, the Privacy Rule states that "[a] covered entity may not use or disclose protected health information . . ."[58] Thus, the Privacy Rule focuses on the offending party's conduct as opposed to the injured party's rights. This language is similar to that contained in FERPA, which the *Gonzaga* court held did not contain rights-creating language.[59] Since the Privacy Rule is

55. Gonzaga Univ. v. Doe, 536 U.S. 273, 287 (2002).

56. *Id.* at 284.

57. Title VI provides that "[n]o person in the United States shall . . . be subjected to discrimination under any program or activity receiving Federal financial assistance." 42 U.S.C. § 2000d (2005). Title IX provides that "[n]o person in the United States shall, on the basis of sex . . . be subjected to discrimination under any education program or activity receiving Federal financial assistance." 20 U.S.C. § 1681(a) (2005).

58. 45 C.F.R. § 164.502(a) (2006).

59. FERPA provides that "[n]o funds shall be made available . . . to any educational agency or institution which has a policy or practice of permitting the release of education records . . . ." 20 U.S.C. § 1232g(b)(1) (2006). Compare this with HIPAA's privacy rule, which provides that "[a] covered entity may not use or disclose protected health information . . . ." 45 C.F.R. § 164.502(a) (2006).

phrased in terms of an obligation imposed on health care providers and, as such, does not explicitly give patients an individual right to privacy, it seemingly cannot be enforced under § 1983.

2. After *Gonzaga*, Can Agency Regulations Ever Be Enforced by § 1983?

In light of *Gonzaga*, some commentators have questioned whether any regulations promulgated by administrative agencies—as opposed to direct congressional legislation—can ever carry the sort of congressional intent that *Gonzaga* requires for § 1983 enforcement.[60] The uncertainty lies in whether Congress intended to create a federal right when it did not write the regulation itself, but instead delegated that authority to an administrative agency. For instance, HHS could have used rights-creating language when it created the Privacy Rule, phrasing it "in terms of the person benefited,"[61] instead of "in terms of institutional policy and practice,"[62] but it is not clear that this would be enough to impute the congressional intent necessary for § 1983 enforcement. It is doubtful that administrative agencies can be considered to speak for Congress. Therefore, it is possible that no administrative regulation, including the Privacy Rule, survives *Gonzaga* to allow for § 1983 enforcement.

Since § 1983 allows for the private enforcement of "rights . . . secured by the Constitution and laws,"[63] the inquiry is two-fold. Courts must ask (1) whether regulations are "laws," and (2) whether regulations can secure federal "rights." Circuit courts have split on the first question,[64] but there is at least some support for the proposition that a regulation may have the "force and effect of law" sufficient for § 1983 enforcement. [65] In *Chrysler Corporation v. Brown*, the Supreme Court held that an agency regulation would carry the "force and effect of law" if it was a substantive rule, properly promulgated under congressional authority.[66]

---

60. Andrew L. Campbell, *Can Federal Regulations Ever Create Federal Rights Privately Enforceable Under Section 1983?*, 38 IND. L. REV. 727, 728 (2005).

61. *Gonzaga*, 536 U.S. at 284 (quoting Cannon v. Univ. of Chi., 441 U.S. 677, 692 n.13 (1979)).

62. *Id.* at 288.

63. 42 U.S.C. § 1983 (2005).

64. *See* Campbell, *supra* note 60, at 739-40 (analyzing the circuit split on whether regulations can be enforced under Section 1983).

65. Chrysler Corp. v. Brown, 441 U.S. 281, 295 (1979).

66. *Id.* at 301-02. Following this analysis, the Court in *Wright v. City of Roanoke Redevelopment & Housing Authority* declared that certain Housing and Urban Development ("HUD") regulations were enforceable under Section 1983. Wright v. City of Roanoke

However, *Gonzaga* arguably precludes the enforcement of agency regulations through § 1983 in the second half of the inquiry—whether regulations can secure federal "rights." In *Alexander v. Sandoval*, the Supreme Court held that regulations promulgated by the Department of Justice pursuant to Title VI of the Civil Rights Act of 1964 did not create an implied private right of action.[67] Writing for the majority, Justice Scalia declared that "it is most certainly incorrect to say that language in a regulation can conjure up a private cause of action that has not been authorized by Congress."[68] Thus, *Sandoval* held that an implied right of action could only be derived from the enabling statute, and not from the regulation itself.

Gonzaga seems to have extended this holding beyond implied right of action cases and into the realm of § 1983 analysis. The *Gonzaga* Court explicitly stated that "our implied right of action cases should guide the determination of whether a statute confers rights enforceable under § 1983."[69] Under this line of reasoning, courts should follow *Sandoval* (an implied right of action case) in determining whether regulations can secure federal rights—a question *Sandoval* answers with a resounding "no." Therefore, *Gonzaga* apparently supports the proposition that only Congress, and not an agency, can create individual rights that are enforceable under § 1983. If this is true, agency regulations, including those promulgated under HIPAA, cannot be enforced through § 1983, even if they otherwise appear to create an unambiguously conferred right.

Regardless of whether *Gonzaga* precludes agencies in all instances from creating individual rights, the Privacy Rule's unique legislative history may itself rule out any possibility of rights creation in this particular case. When it enacted HIPAA in 1996, Congress did not originally grant HHS the authority to promulgate the regulations that we now know as the Privacy Rule. Rather, HIPAA required Congress itself to promulgate comprehensive privacy legislation within three years.[70] HIPAA only granted HHS the authority to step in and issue its own privacy regulations in the event that Congress failed to act within this time frame.[71] After three years of Congressional inactivity, HHS undertook the task of promulgating the

---

Redevelopment & Housing Authority, 479 U.S. 418, 431 (1987) (holding that HUD regulations carried "the force of law", thereby conferring an enforceable right to plaintiffs).

67. Alexander v. Sandoval, 532 U.S. 275, 293 (2001).

68. *Id.* at 291.

69. *Gonzaga*, 536 U.S. at 283.

70. 42 U.S.C. § 1320d-2 note (Pub. L. No. 104-191 § 264(c)(1)).

71 *Id.*

Privacy Rule by default.[72] This situation is substantially unlike the traditional case of Congress explicitly authorizing an agency to promulgate regulations. When Congress enacted HIPAA, it fully intended to write the Privacy Rule itself, not to allow the agency to act on its behalf. Congress's failure to meet its own deadline cannot be interpreted to carry the same degree of deferral to the agency as if it had explicitly granted this authority at the outset. This unique legislative history draws into question how much authority HHS should be assumed to have, and whether it is proper to read these regulations as being indicative of any degree of congressional intent. Any suggestion of an individual right in HHS's Privacy Rule certainly cannot be imputed to Congress under these unusual circumstances.

3. *Abrams* Might Also Preclude § 1983 Enforcement of the Privacy Rule

Even if the Privacy Rule passed the *Gonzaga* test, it would face another barrier to § 1983 enforcement in *City of Rancho Palos Verdes v. Abrams*.[73] The Court in *Abrams* held that statutes containing an independent judicial remedy could not be enforced by § 1983.[74] The specific provision at issue in *Abrams* provided for a *judicial* remedy.[75] Therefore, there is some question as to whether or not an *administrative* remedy, such as that provided for in HIPAA, would act to preclude § 1983 actions in the same way. However, dicta in the opinion suggest that the presence of an administrative remedy would have a similar effect. Justice Scalia noted that "in *all* of the cases in which we have held that § 1983 *is* available for violation of a federal statute, we have emphasized that the statute at issue . . . *did not* provide a private judicial remedy (or, in most of the cases, even a private administrative remedy) for the rights violated."[76]

HIPAA's privacy regulations contain a fairly detailed enforcement scheme. Although the Privacy Rule does not allow affected persons to seek individual redress, it does allow individuals to

---

[72] Jennifer Guthrie, *Time Is Running Out - The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the "Minimum Necessary" Standard, and the Notice of Privacy Practices*, 12 ANNALS HEALTH L. 143, 145 n.8 (2003).

73. City of Rancho Palos Verdes v. Abrams, 544 U.S. 113 (2005).

74. *Id.* at 127.

75. The TCA provides: "Any person adversely affected by any final action or failure to act by a State or local government or any instrumentality thereof that is inconsistent with this subparagraph may, within 30 days after sucb action or failure to act, commence an action in any court of competent jurisdiction." 47 U.S.C. § 332(c)(7)(B)(v) (2005).

76. *Abrams*, 544 U.S. at 121.

file complaints against non-compliant entities.[77] Furthermore, HHS can commence compliance reviews to determine whether an entity is in compliance with HIPAA regulations.[78] The regulations are enforced through a scheme of both civil fines and criminal punishment. As a civil matter, the Secretary may fine anyone who violates HIPAA not more than $100 per violation, up to a total of $25,000 per year for all violations of a single regulation.[79] As a criminal matter, anyone who knowingly uses, obtains, or discloses identifiable health information can be fined up to $50,000 or imprisoned for up to one year.[80] A person who commits an offense "under false pretenses" may be subject to fines up to $100,000 and imprisonment up to five years[81] and a person who commits an offense "for commercial advantage, personal gain, or malicious harm" may be subject to fines up to $250,000 and up to ten years imprisonment.[82]

Abrams suggests that the administrative remedies provided in the HIPAA regulations might be enough to preclude the use of § 1983 as a vehicle for statutory enforcement since such an action "would distort the scheme of . . . limited remedies" found within the statute.[83] Therefore, plaintiffs seeking to bring § 1983 actions for Privacy Rule violations face significant hurdles in both *Gonzaga* and *Abrams*. Since the Supreme Court's trend toward limiting § 1983's scope severely limits the ability of plaintiffs to bring these suits, patients whose medical privacy rights have been violated must look elsewhere for a possible right of action.

III. FALSE CLAIMS ACT

A. Background

The False Claims Act ("FCA") is a civil statute designed "to protect government funds and property from fraudulent claims."[84] Originally passed in 1863 to prevent the fraudulent use of government funds during the Civil War,[85] the FCA imposes liability upon "[a]ny

77. 45 C.F.R. § 160.306(a) (2006). HHS provides a Health Information Privacy Complaint form that can be retrieved online at http://www.hhs.gov/ocr/howtofileprivacy.pdf (last visited Jan. 27, 2006).

78. 45 C.F.R. § 160.308 (2006).

79. 42 U.S.C. § 1320d-5(a) (2000).

80. 42 U.S.C. § 1320d-6(b)(1) (2000).

81. 42 U.S.C. § 1320d-6(b)(2) (2000).

82. 42 U.S.C. § 1320d-6(b)(3) (2000).

83. City of Rancho Palos Verdes v. Abrams, 544 U.S. 113, 127 (2005).

84. Costner v. URS Consultants, Inc., 153 F.3d 667, 676 (8th Cir. 1998).

85. United States v. Neifert-White Co., 390 U.S. 228, 232 (1968).

person who knowingly presents, or causes to be presented, to an officer or employee of the United States Government . . . a false or fraudulent claim for payment or approval . . . ."[86] Thus, the elements that must be proved to establish a violation of the False Claims Act are: (1) the defendant presented or caused a third party to present a claim to the government, (2) the claim was false or fraudulent, and (3) the defendant acted knowingly. FCA claims may be brought by the Department of Justice or by private parties acting as "whistleblowers."[87] In these so-called qui tam actions,[88] a private party (or "relator") is authorized to bring a suit on behalf of the government and, if successful, may share in the potentially large recovery.[89]

The FCA has recently gained popularity among plaintiffs as a way to bring claims of health care fraud against entities that receive government benefits in the form of Medicare and Medicaid funds.[90] Although creative plaintiffs could conceivably adapt the various theories used to support FCA enforcement of health care fraud to the Privacy Rule context, this Note will argue that such a theory would be contrary to congressional intent and would have a negative impact on the provision of medical services as a whole. Before this argument can be made, however, it is necessary to dissect the various theories of the FCA, particularly as they have developed as a weapon to combat health care fraud and abuse.[91]

1. Getting to Implied False Certification: Theories of FCA Enforcement

The most basic application of the False Claims Act occurs when the claim for federal funds itself is factually false.[92] In such cases, the

86. 31 U.S.C. § 3729(a) (2000).

87. 31 U.S.C. § 3730(a)-(b) (2000).

88. The term comes from the Latin "*Qui tam pro domino rege quam pro sic ipso in hoc parte sequitur*," which means, "who as well for the king as for himself sues in this matter." BLACK'S LAW DICTIONARY 1282 (8th ed. 2004).

89. An unsuccessful FCA defendant may be liable to the government for up to $10,000 in civil fines, plus treble damages. 31 U.S.C. §3729 (2000). Qui tam plaintiffs are eligible to receive up to 30 percent of the government's total recovery, plus court costs and attorneys' fees. 31 U.S.C. §3730(d) (2000).

90. *See* Lisa Michelle Phelps, Note, *Calling Off the Bounty Hunters: Discrediting the Use of Alleged Anti-Kickback Violations to Support Civil False Claims Actions*, 51 VAND. L. REV. 1003, 1004 (1998) ("[G]overnment prosecutors and private parties are frequently turning to the Civil False Claims Act as their weapon of choice in waging the 'war' on health care fraud and abuse.").

91. The health care fraud and abuse laws include the Anti-Self-Referral ("Stark") law, 42 U.S.C.A. §1395nn (2005), and the Anti-Kickback law, 42 U.S.C.A. § 1320a-7b (2005).

92. *See, e.g.*, United States v. Neifert-White Co., 390 U.S. 228, 230 & n.2 (1968) (holding that a grain dealer who furnished false invoices, which overstated the purchase price of the bins of grain he sold, was expressly within the reach of the False Claims Act).

plaintiff need only present some objective evidence showing that the information on the defendant's claim was inaccurate and that the defendant knew or should have known that this was the case. This straightforward theory of the FCA applies in the health care setting when a provider submits a claim for federal Medicaid or Medicare funds for services that it never provided[93] or for services that were not medically necessary.[94]

One step removed from this traditional application of the FCA is the theory of "false certification," which has recently developed to allow private parties to enforce health fraud laws. Under this theory, a claim is false when it "falsely certifies compliance with a particular statute, regulation or contractual term, where compliance is a prerequisite to payment."[95] Therefore, the claim is considered to be false not because of the substantive information included in the claim itself, but because of its false representation of compliance. The claim is legally false even though the medical services claimed for reimbursement were provided and were medically necessary.

"False certification" allows liability to attach even though the government has not suffered a cognizable pecuniary loss. *United States ex rel. Pogue v. American Healthcorp, Inc.* held that the FCA does not require actual damage to the government.[96] Instead, the plaintiff need only show that the government made payments to an unworthy recipient.[97] The district court reasoned that the FCA was "intended to govern not only fraudulent acts that create a loss to the government but also those fraudulent acts that cause the government to pay out sums of money to claimants it did not intend to benefit."[98] Under this theory, there need not be a nexus between the statute that is being ignored and the activity for which payment is being claimed since, theoretically, the violation of any regulation or statute could make a claim "false" if compliance with that law was a prerequisite to payment.[99]

---

93. *See* United States v. Lorenzo, 768 F.Supp. 1127, 1130-31 (E.D. Pa. 1991) (holding defendant dentist liable under the FCA for submitting claims for certain oral examinations as "limited consultations" when they were in fact simply routine dental examinations).

94. *See In re* Cardiac Devices Qui Tam Litig., 221 F.R.D. 318, 334-36 (D. Conn. 2004) (holding that, if a hospital billed Medicare for procedures that were not reasonably necessary, tbis would constitute fraudulent conduct under the FCA).

95. Mikes v. Straus, 274 F.3d 687, 698 (2d Cir. 2001).

96. United States *ex rel.* Pogue v. Am. Healthcorp, Inc., 914 F.Supp. 1507, 1509, 1513 (M.D. Tenn. 1996).

97. *Id.* at 1513.

98. *Id.*

99. The "false certification" tbeory has gained traction in other jurisdictions, as well. For example, the Fifth Circuit tentatively accepted *Pogue's* reasoning in *United States* ex rel. *Thompson v. Columbia/HCA Healthcare Corporation.* United States *ex rel.* Thompson v.

The "implied false certification" theory (also called the "tainted claim" theory) extends the False Claims Act one step further. An implied false certification claim is "based on the notion that the act of submitting a claim for reimbursement itself implies compliance with governing federal rules that are a precondition to payment."[100] Under this theory, no explicit statement of compliance is required because the defendant has an affirmative obligation to ensure that it follows the law. Simply by submitting the claim, the defendant impliedly certifies compliance with all applicable regulations.

Unlike the express false certification theory, the implied false certification theory requires some nexus between the alleged non-compliance and the activity for which payment is claimed.[101] For example, a claim for Medicare reimbursement does not violate the False Claims Act simply because the hospital does not comply with a local zoning ordinance. There must be some relation between the claim for federal funds and the regulation that is not being followed. In the health fraud setting, plaintiffs argue that this nexus is satisfied because providers that receive Medicare and Medicaid funds have an obligation to ensure compliance with all HHS regulations.[102]

Furthermore, the FCA requires that the defendant have actual knowledge that the claim is false, or must deliberately ignore or recklessly disregard this fact.[103] The FCA's scienter requirement is completely independent of the scienter requirement imposed by the underlying statute or regulation that has allegedly placed the defendant in a position of non-compliance. This effectively creates a dual scienter requirement for FCA claims. First, the plaintiff must prove that the defendant had the requisite intent to establish a violation of the underlying statute, and then must prove that the defendant also had knowledge that the certification of compliance was false.

Columbia/HCA Healthcare Corporation, 125 F.3d 899 (5th Cir. 1997). The court stated that "where the government has conditioned payment of a claim upon a claimant's certification of compliance with, for example, a statute or regulation, a claimant submits a false or fraudulent claim when he or she falsely certifies compliance with that statute or regulation." *Id.* at 902. Thus, *Thompson* seems to allow recovery under the FCA even when the claimed services were appropriately rendered, depending on the nature of the certification required for payment.

100. *Mikes*, 274 F.3d at 699.

101. *See* Phelps, *supra* note 87, at 1015-16 (noting that the FCA theory of implied false certification requires courts to analyze "whether a relation exists between the subject matter of the false statement and the government's loss").

102. *See id.* at 1016 n.60 (remarking that this implied obligation probably stems from statements made in the 1986 Senate Report that "those doing business with the Government have an obligation to make a limited inquiry to ensure the claims they submit are accurate" (quoting S. REP. NO. 99-345, at 7 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 5266, 5272)).

103. 31 U.S.C. § 3729(b) (2000).

2. Advantages of the FCA

The FCA has become an attractive tool for plaintiffs to bring suits against health care entities for several reasons. First, it allows plaintiffs to sue under statutes that do not themselves create a private right of action. For instance, despite the fact that neither the Anti-Self-Referral ("Stark") law[104] nor the Anti-Kickback law[105] provides a private cause of action, plaintiffs have been able to use the qui tam provisions of the FCA to prosecute alleged violations of both of these statutes.[106]

Second, the FCA affords plaintiffs certain evidentiary advantages. Plaintiffs that use the FCA to prosecute fraud under the Stark or Anti-Kickback laws bear only a civil burden of proof and therefore need only show that the fraudulent activity occurred by a preponderance of the evidence, rather than beyond a reasonable doubt as would be required in a criminal fraud prosecution brought under either of these laws independently.[107] Additionally, the FCA requires no showing that a defendant's violation of the statute harmed the government.[108]

The only potential evidentiary hurdle imposed on FCA plaintiffs is the "original source" requirement, which states that the whistleblower must be the "original source" of the information upon which the FCA claim is based; claims cannot be based on information that has already been publicly disclosed.[109] However, even this limitation may be relatively inconsequential since some courts have been quite permissive in who they determine to be an "original source."[110]

The potential for large recoveries makes the False Claims Act an attractive option for would-be plaintiffs. Anyone found in violation of the FCA may be liable for both treble damages and a "per claim" civil penalty of up to $10,000.[111] Furthermore, these civil penalties damages are to some extent mandatory. The FCA requires courts to

---

104. 42 U.S.C.A. § 1395nn (2005).

105. 31 U.S.C. § 3729 (2000).

106. *See, e.g.*, United States *ex rel.* Pogue v. Am. Healthcorp, Inc., 914 F. Supp. 1507, 1513 (M.D. Tenn. 1996) (holding that the plaintiff can bring a claim alleging violations of the anti-kickback and anti-self-referral laws under the False Claims Act).

107. United States v. JT Constr. Co., 668 F. Supp. 592, 593 (W.D. Tex. 1987).

108. *Pogue*, 914 F. Supp. at 1513.

109. 31 U.S.C. § 3730(e)(4)(A) (2000).

110. *See, e.g.*, United States *ex rel.* Schumer v. Hughes Aircraft Co., 63 F.3d 1512, 1518 (9th Cir. 1995), *rev'd on other grounds*, 520 U.S. 939 (1997) (holding that disclosure to employees or potential availability to the public through the Freedom of Information Act does not constitute "public disclosure.").

111. 31 U.S.C. § 3729(a) (2000).

impose civil penalties of at least $5000 and states that "the court may assess not less than 2 times the amount of damages which the government sustains because of the act of the person."[112] Since "per claim" has been interpreted to mean "per line item" and not "per bill," total recoveries in these cases have reached into the millions of dollars.[113] The private plaintiffs that bring these qui tam actions under the FCA could be awarded as much as thirty percent of the government's total recovery, as well as all costs and attorneys' fees.[114] Therefore, successful plaintiffs stand to receive recoveries in the millions of dollars without necessarily having suffered any actual harm themselves.[115] Clearly, the FCA's procedural and financial advantages make it an attractive option for plaintiffs seeking to bring suit under a statute that does not provide its own private right of action.

B. Using the FCA to Enforce the Privacy Rule

The Privacy Rule generally prohibits covered entities from disclosing "protected health information"[116] except in certain situations.[117] This broad prohibition has created vast amounts of potentially illegal activity, including within its scope a host of seemingly benign actions.[118] As a result, most hospitals are willing to admit that they are not fully compliant with HIPAA regulations.[119]

---

112. *Id.*

113. *See* Michael Pretzer, *Why You Should Have Been at the Health Lawyers' Convention, National Health Lawyers Association's 1996 Conference*, MED. ECON., Aug. 26, 1996, at 160, 166 (explaining how the FCA can multiply modest actual damages into multimillion-dollar judgments). For example, HealthSouth recently agreed to pay the US government $325 million to settle allegations of Medicare fraud in a case brought as a qui tam action under the FCA. *HealthSouth Agrees to Pay $325 Million to Resolve Medicare Billing Allegations*, 14 HEALTH L. REP. 25 (2005).

114. 31 U.S.C. § 3730(d)(2) (2005).

115. The two qui tam plaintiffs in the HealthSouth case will receive $8.1 million and $4 million respectively. *HealthSouth*, *supra* note 110, at 25.

116. Protected health information is defined as "individually identifiable health information" that is "[t]ransmitted or maintained in any form or medium." 45 C.F.R. § 160.103 (2006).

117. 45 C.F.R. § 164.502(a) (2006).

118. For example, numerous Privacy Rule violations occur every day when hospital visitors overhear hallway conversations between doctors and nurses. *Hallway Talk Can Violate HIPAA Privacy Rule*, 13 REHAB CONTINUUM REP. 117 (2004).

119. In a recent survey, only 40.3% of health care providers indicated that they are in full compliance with HIPAA regulations. AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, THE STATE OF HIPAA PRIVACY AND SECURITY COMPLIANCE 11 (2005), *available at* http://www.ahima.org/marketing/email_images/2005PrivacySecurity.pdf. One year after the compliance deadline for hospitals and health plans, 4% have indicated that they are less than 50% compliant. *Id.* As of August 31, 2005, the HHS Office for Civil Rights had received 15,000 HIPAA privacy complaints and had trained 200 regional investigators to handle the additional 600 new complaints that the office receives on average each month. *Health Information*

Considering the way the FCA has been significantly expanded in the context of health care fraud, it seems quite possible that plaintiffs could use the developing false certification theory to enforce Privacy Rule violations. However, the results of allowing this type of suit to go forward would be staggering, since each of the minor Privacy Rule violations that occur on a daily basis would represent a potential lawsuit.

A plaintiff attempting to establish a cause of action under the FCA for a Privacy Rule violation must prove two major elements. First, the plaintiff must show that the covered entity either expressly or impliedly certified compliance with HIPAA regulations. The plaintiff may be able to point to an actual representation of compliance since Medicare laws expressly require claimants to certify compliance with all federal laws.[120] However, even absent evidence that claimants have expressly certified compliance, the plaintiff could proceed under the implied false certification theory by arguing that Medicaid hospitals have an affirmative duty to ensure compliance with all HHS regulations.[121]

Second, the plaintiff must prove that a recent Privacy Rule violation made the representation of compliance legally false. In the current health care climate, where Privacy Rule violations occur on a regular basis, this second requirement would be easily met. Any time a covered entity commits a Privacy Rule violation, it places itself in a position of non-compliance with HIPAA regulations; therefore, any subsequent claim for Medicare or Medicaid reimbursement would

---

Privacy/Security Alert Focuses on HHS Referrals of HIPAA Privacy Complaints to Other Federal, State Regulators; Oct. 12 Audio Seminar Helps Healthcare Cope with Government Investigations, BUSINESS WIRE, Oct. 3, 2005, *available at* Thomson Gale PowerSearch, Doc. No. A136993494.

120. The administrator or chief financial officer must certify compliance with Medicare laws in the hospital's annual cost report. The regulations set forth the procedures related to the filing of annual cost reports for Medicare and states that:

> The following statement must immediately precede the dated signature of the provider's administrator or chief financial officer: I hereby certify that I have read the above certification statement and that I bave examined the accompanying electronically filed or manually submitted cost report and the Balance Sheet Statement of Revenue and Expenses prepared by ____ (Provider Name(s) and Number(s)) for the cost reporting period beginning ____ and ending ___ and that to the best of my knowledge and belief, this report and statement are true, correct, complete and prepared from the books and records of the provider in accordance with applicable instructions, except as noted. I further certify that I am familiar with the laws and regulations regarding the provision of health care services, and that *the services identified in this cost report were provided in compliance with such laws and regulations*.

42 C.F.R. 413.24 (2006) (emphasis added).

121. *See supra* text accompanying note 97.

involve a false certification of compliance with all applicable laws and would constitute a false claim.

C. Arguments Against FCA Enforcement of the Privacy Rule

1. FCA Enforcement of Privacy Rule Violations Could Lead to a Flood of Litigation

Key differences exist between health care fraud and abuse laws and HIPAA's Privacy Rule regarding their potential for FCA enforcement, suggesting that FCA enforcement of the Privacy Rule may not be desirable. Specifically, some of the limitations attached to FCA enforcement of fraud would not be as effective in limiting the use of the FCA to enforce the Privacy Rule. If aggressive qui tam plaintiffs were able to enforce minor Privacy Rule violations, the result could be a dramatic increase in medical privacy litigation. Failing to limit these actions could have a net adverse effect on patients since heath care providers would be forced to spend limited resources defending claims, rather than treating patients. Furthermore, fear of liability may lead to over-deterrence in the health care system, which could have a negative impact on the standard of care provided to patients. Over-burdening of courts could also affect legitimate plaintiffs by delaying adjudication of even the most valid claims.

The FCA's dual scienter requirement acts as gatekeeper in the health fraud context, limiting the potential number of claims by imposing a higher burden of proof on potential qui tam plaintiffs.[122] In contrast, there would be no dual scienter requirement for FCA enforcement of the Privacy Rule since non-criminal HIPAA violations do not carry any specific scienter requirement.[123] Covered entities violate the Privacy Rule any time they improperly disclose protected health information, regardless of whether such disclosure was intentional, negligent, or entirely innocent. Therefore, every minor Privacy Rule violation places the covered entity in a position of non-compliance with HIPAA regulations, automatically making any

122. *See* discussion *supra* Section III(A)(i), noting that the plaintiff in an FCA action must prove that the defendant had the requisite intent to establish a violation of the underlying fraud statute as well as the knowledge that a false claim was being submitted to the government so as to satisfy the FCA's separate scienter requirement.

123. Generally, the HHS Secretary may impose civil fines on "*any person* who violates" the Privacy Rule. 42 U.S.C. §1320d-5(a) (2005) (emphasis added). However, there are specific scienter requirements related to the imposition of the various levels of criminal penalties. *See* 42 U.S.C. § 1320d-6 (2005) (establishing increasing criminal penalties for violations committed "knowingly", those committed "under false pretenses", and those committed "for commercial advantage, personal gain, or malicious harm.").

subsequent claim for reimbursement a "false claim." Plaintiffs need only meet the FCA's relatively low burden of proving that the covered entity recklessly disregarded the fact that the claim was submitted despite non-compliance with the Privacy Rule.[124] This should not be exceedingly difficult to prove since health care providers are apparently aware of the fact that they are not fully compliant with HIPAA's regulations.[125]

The only remaining limitation on qui tam actions is the FCA's "original source requirement," which states that the plaintiff must have "direct and independent knowledge of the information on which the allegations are based . . . ."[126] This requirement can substantially limit the ability of qui tam plaintiffs to bring actions for health fraud since those allegations are based on information that is not generally accessible to patients.[127] In contrast, most Privacy Rule enforcement cases would easily meet the "original source" requirement because the patient is likely to be the first to discover that his or her protected health information was disclosed without permission.[128] In these cases, the "direct and independent knowledge" requirement would not seem to pose a significant limitation on a plaintiff's ability to bring a qui tam action.

When one combines the absence of limitation in pursing FCA claims for Privacy Rule violations with the advantages the FCA affords plaintiffs generally—especially the potential for large financial recoveries[129]—the incentives for plaintiffs to bring such actions are great. This could lead to a flood of litigation with the potential to cripple the health care industry.

---

124. 31 U.S.C. § 3729(b) (2005).

125. *See* AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, *supra* note 119, at 11 (reporting that a majority of hospitals admit that they are not fully compliant with HIPAA regulations despite the fact that the deadline for full compliance has already passed).

126. 31 U.S.C. § 3730(e)(4) (2005).

127. In order to prove an anti-kickback violation, the plaintiff must have direct and independent knowledge that the defendant used remuneration to induce referrals. *See* 42 U.S.C § 1320a-7b(b) (2005) (prohibiting the solicitation, receipt, offer, or payment of remuneration in return for referrals). Stark violations pose an even greater hurdle since the plaintiff must have direct and independent knowledge of the financial and ownership structure of the health care provider. *See* 42 U.S.C. § 1395nn(a) (2005) (prohibiting physicians from making referrals to an entity with which they have a "financial relationship").

128. Covered entities are permitted to release protected health information when the patient consents. 45 C.F.R. § 164.502(a)(1)(v) (2006). Since the appropriateness of the disclosure depends on the patient's desires, the patient is uniquely well situated to determine when and if the Privacy Rule has been ignored. Therefore, the patient is more likely to be the original source of this information than the federal government or the any other party.

129. *See supra* notes 109-13 and accompanying text.

2. The Supreme Court's Policy of Limiting § 1983 Actions Should Apply to FCA Actions by Analogy

At least one commentator has made a comparison between § 1983 and the FCA as structurally similar statutory vehicles.[130] By drawing an analogy between these two statutes, it can be argued that the policy of limiting § 1983 claims is equally compelling in the FCA context; therefore FCA claims should be limited in the same way that § 1983 claims have been limited in recent years.[131]

Both § 1983 and the FCA allow parties to bring private actions for violations of separate statutes that do not themselves provide private causes of action. The Supreme Court has recently demonstrated a reluctance to allow parties to bring § 1983 claims.[132] Under a § 1983 analysis, courts must analyze the underlying statute to determine whether Congress intended to create an unambiguously conferred federal right.[133] The existence of a comprehensive enforcement scheme in the statute itself provides a further limitation on § 1983's availability.[134] Since the Privacy Rule would presumably fail to meet these requirements, private parties would not be able to bring a § 1983 claim to enforce a Privacy Rule violation.[135] Parties should not be able to usurp the policies that the Supreme Court has advanced by resorting to the FCA as an alternative statutory vehicle in order to circumvent the barriers imposed by § 1983.

3. FCA Enforcement of Privacy Rule Violations Undermines Congressional Intent

FCA enforcement of Privacy Rule violations should be precluded if such enforcement would undermine congressional intent. In *Aetna Health, Inc. v. Davila*,[136] the Supreme Court held that an action brought under a Texas law was completely pre-empted by the Employee Retirement Income Security Act ("ERISA"), regardless of whether or not the state law fell within an exception to preemption.[137] Justice Thomas reasoned that "[a]llowing respondents to proceed with

130. Phelps, *supra* note 90, at 1033-36.

131. *See id.* (arguing that the statutes' structural similarity supports the use of Section 1983's analytical tools to evaluate False Claims actions).

132. *See* discussion *supra* Section II.B (analyzing the Supreme Court's trend towards the restriction of Section 1983 claims).

133. Gonzaga Univ. v. Doe, 536 U.S. 273, 283-84 (2002).

134. City of Rancho Palos Verdes v. Abrams, 544 U.S. 113, 126-27 (2005).

135. See *discussion supra* Section II.C (arguing that the Privacy Rule would fail the tests for Section 1983 enforceability set forth by the Supreme Court in *Gonzaga* and *Abrams*).

136. Aetna Health, Inc. v. Davila, 542 U.S. 200 (2004).

137. *Id.* at 221.

their state-law suits would 'pose an obstacle to the purposes and objectives of Congress."[138] Extending this principle to the present situation, a Privacy Rule violation should not be enforced through the FCA if such an action would conflict with HIPAA's purposes and objectives. Even though *Aetna* does not demand this result (the conflicting statute in that case was a state law, whereas the conflicting statute here—the FCA—is a federal statute), Justice Thomas's concern is no less applicable in this situation. Courts should not stretch the FCA so far beyond its original application as to undercut Congress' intent in establishing HIPAA.[139] Therefore, the analysis centers on whether qui tam enforcement of Privacy Rule violations would undermine congressional intent. This type of question rarely yields a clear answer, but current indications are that Congress did not intend to create a private right of action for Privacy Rule violations.

Congress undoubtedly contemplated private enforcement of the Privacy Rule during HIPAA's formative years; therefore, the absence of private enforcement language in the final regulations should not be seen as an inadvertent omission, but a conscious choice. In a 1997 statement to the Senate Committee on Labor and Human Resources, HHS Secretary Donna Shalala made the following remarks:

> We believe that any individual whose rights under the federal privacy law have been violated—whether those rights were violated negligently or knowingly—should he permitted to bring a legal action for actual damages and equitable relief. When the violation was done knowingly, attorney's fees and punitive damages should be available.[140]

Three years later, a White House press release echoed this sentiment, stating that "[a]lthough these [administrative] enforcement provisions will be helpful, they are no substitute for a private right of action, which makes it possible for patients to be compensated for harmful plan actions."[141] Commentators writing at the time also noted

---

138. *Id.* at 217 (quoting Pilot's Life Ins. Co. v. Dedeaux, 481 U.S. 41, 52 (1987)).

139 The utility of this analogy should not be overstated. Congress may not have intended the Privacy Rule to be as exclusive and comprehensive as ERISA, and therefore the need to protect it from circumvention through other avenues is arguably not as strong as in the case of ERISA. It is clear, however, that the Privacy Rule was intended to create a uniform baseline of medical record protection. Courts should protect congressional intent as to the enforcement of this law to prevent the emergence of liability that was never envisioned under this scheme.

140. *Protecting our Personal Health Information: Privacy in the Electronic Age: Hearing Before the S. Comm. on Labor & Human Resources*, 105th Cong. 23 (1997) (statement of Donna Shalala, Secretary of Health & Human Services).

141. Press Release, White House, President Clinton Issues Strong New Consumer Protections to Ensure the Privacy of Medical Records (Dec. 20, 2000), *available at* 2000 WL 1863510.

the possibility that a private right of action could stem from these regulations.[142]

However, any suggestion that HIPAA's legislative history supports private enforcement is undercut by the fact that the regulations clearly establish a scheme of civil and criminal penalties enforceable solely by the HHS Secretary.[143] Even though HHS supports the development of a private right of action,[144] it has deferred to Congress on this issue.[145] Despite the recommendations of HHS and others, Congress's response has been one of inaction. Furthermore, courts have consistently refused to recognize a private right of action under HIPAA.[146] If Congress desires this statute to be interpreted to provide a private right of action then it must say so, which it has declined to do thus far.

Moreover, HHS's use of prosecutorial discretion in determining when to impose civil penalties on offending parties suggests that the Privacy Rule's highly technical regulations were intended to be under-enforced. HHS has stated that "a covered entity will not necessarily suffer a penalty solely because an act or omission violates the rule."[147] Instead, "the Department will exercise discretion to consider not only the harm done, but the willingness of the covered entity to achieve voluntary compliance."[148] Such intentional under-enforcement supports HHS's position that the Privacy Rule's purposes and objectives are best served by focusing on achieving voluntary compliance by providing technical assistance and educational programs rather than by strictly enforcing the regulations by issuing fines.[149]

---

142. *See* Chad Bowman, *Anticipated Privacy Rule Could Give Tort Lawyers New Weapon, Some Say*, 9 HEALTH L. REP. 1852 (2000) (reporting predictions that plaintiffs could potentially use HIPAA to bring tort claims, contract claims, federal trade claims, or FCA claims).

143. 42 U.S.C. § 1320d-5, 6 (2005).

144. "[W]e believe that . . . federal law should allow any individual whose rights have been violated to bring an action for actual damages and equitable relief. The Secretary's Recommendations, which were submitted to Congress on September 11, 1997, called for a private right of action to permit individuals to enforce their privacy rights." 65 Fed. Reg. 82462, 82605 (Dec. 28, 2000).

145. "We agree [that individuals should be able to sue for breach of privacy], but do not have the legislative authority to grant a private right of action to sue under this statute. Only Congress can grant that right." 65 Fed. Reg. at 82566.

146. *See* Runkle v. Gonzales, 391 F. Supp. 2d 210, 237-38 (D.D.C. 2005) (dismissing plaintiff's HIPAA claim on the grounds that HIPAA does not create a private right of action); Johnson v. Quander, 370 F. Supp.2d 79, 100 (D.D.C. 2005) (same); O'Donnell v. Blue Cross Blue Shield of Wyoming, 173 F. Supp.2d 1176, 1179 (D. Wyo. 2001) (same).

147. 65 Fed. Reg. 82462, 82603 (Dec. 28, 2000).

148. *Id.*

149. 65 Fed. Reg. at 82604. Prosecutors also used discretion in their enforcement of health fraud laws by ignoring many of the benign, technical violations and instead targeting only the most egregious violations. In that sense, the health care industry has been called "a speakeasy,

Allowing private parties to bring actions under the FCA would clearly frustrate the Privacy Rule's purpose. Qui tam plaintiffs acting in their own self-interest cannot be expected to exercise the same prosecutorial discretion as that which is exercised by the HHS Secretary. Qui tam enforcement of Privacy Rule violations would lead to suits based on technical violations for harmless activity that HHS never intended to prosecute when it promulgated these regulations. When one considers the countless number of benign violations that occur in large hospitals every day,[150] it becomes apparent that such enforcement could lead to a proliferation of suits brought by aggressive qui tam plaintiffs. The threat of such litigation would stifle the medical community and could conceivably lead to a decrease in the quality of care that these entities provide.[151] It seems clear that FCA enforcement of the Privacy Rule would conflict with the purposes and objectives that Congress intended HIPAA to achieve.

IV. SOLUTION: ENFORCEMENT OF PRIVACY RULE VIOLATIONS THROUGH TORT LAW

The Supreme Court has limited § 1983's scope in recent years, ostensibly foreclosing a patient's ability to bring § 1983 actions for Privacy Rule violations. Although FCA enforcement remains possible, the incentives created by such an action could lead to a proliferation of suits brought against health care providers, which could have a negative effect on the quality of treatment that patients receive. However, this should not lead to the conclusion that the Privacy Rule is best left under-enforced, thereby barring injured patients from bringing a private cause of action against the responsible party. Medical privacy violations are a very serious issue that must be dealt with in order to adequately protect patients' privacy rights and to restore confidence in the health care system.[152] Therefore, it is necessary to strike a balance between two competing interests: the interest of allowing injured patients to recover for wrongs committed against them, and the interest of protecting the health care system

---

with wholesale illegal conduct taking place but being winked at by prosecutors" who will only prosecute "the loud and obnoxious drunks." James F. Blumstein, *What Precisely is "Fraud" in the Health Care Industry?*, WALL ST. J., Dec. 8, 1997, at A25.

150. *See* discussion *supra* Part III.B (discussing the broad scope of potential Privacy Rule liability created by the existence of numerous minor violations).

151. *See* Charity Scott, *Is Too Much Privacy Bad For Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481, 500-03 (2000) (discussing the various ways in which accessibility, rather than strict confidentiality, of medical records can be used by various healthcare providers to achieve increased efficiency and a higher quality of care for the patient's own benefit).

152 See discussion supra Part I (discussing loss of confidence in the health care system).

from excessive liability. This Note proposes that, absent legislative action, tort law provides the best system in which these interests can be balanced.

Tort law is a system of redress for wrongs.[153] As such, its primary goal is to compensate the plaintiff for harm caused as a direct result of the defendant's breach of a recognized duty.[154] A right of action grounded in tort law would allow plaintiffs who have been legitimately harmed by unauthorized medical records disclosure to recover for their injury, but would not allow unharmed, opportunistic plaintiffs to enforce regulations that should be left to the HHS Secretary's discretion. This would achieve the proper balance of securing justice for patients without subjecting heath care providers to frivolous litigation.

Prior to HIPAA's enactment, courts allowed patients to recover against their physicians for the unauthorized disclosure of confidential medical information. Such recoveries were based on two distinct causes of action: (1) the traditional tort cause of action for invasion of privacy and (2) the physician's breach of his professional duty of confidentiality. This Note argues that courts should analyze medical privacy actions under breach of confidentiality principles. Furthermore, because the Privacy Rule imposes new obligations on health care providers, the underlying duty of care must be reanalyzed in light of these changes to determine how courts should approach medical privacy breaches in the future.

A. Invasion of Privacy

United States common law did not originally contain a right of privacy until a law review article by Samuel Warren and Louis Brandeis eventually led courts to explicitly recognize privacy as a common law right.[155] Tort law currently recognizes four different ways that a person's right of privacy may be invaded: (1) "unreasonable intrusion upon the seclusion of another," (2) "appropriation of the other's name or likeness," (3) "unreasonable publicity given to the other's private life," and (4) "publicity that unreasonably places the other in a false light before the public."[156] Of the four theories of invasion of privacy, only the third theory—unreasonable publicity—

153. JOHN C. P. GOLDBERG, ANTHONY J. SEBOK & BENJAMIN C. ZIPURSKY, TORT LAW: RESPONSIBILITIES AND REDRESS 38 (Aspen Publishers 2004).

154. *Id.* at 3.

155. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (arguing that there exists a right of privacy, the violation of which is a cognizable injury to which the law should provide redress).

156. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

appears to be applicable in the context of medical record disclosures.[157] This cause of action may indeed be of limited use in certain cases; however, it does not provide an adequate means of redress for most medical record disclosures. The Restatement (Second) of Torts states that

> [o]ne wbo gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[158]

This definition of invasion of privacy probably severely limits its applicability to most cases of medical record disclosures for two reasons. First, it is not entirely clear that a general disclosure of medical records would be "highly offensive to a reasonable person." Although some health conditions carry a negative social stigma, making any disclosure potentially offensive to the patient, this is not necessarily true in every case. In many instances, disclosure to strangers with no interest in the information would not be considered offensive. Instead, it is the disclosure of medical records to entities most interested in that information (employers, for example) that can be most devastating to the patient.[159]

Second, the definition of "publicity" limits the applicability of the violation of privacy tort in regards to garden variety medical record disclosures. The Restatement explicitly defines this term as a communication "to the public at large."[160] Thus, invasion of privacy would only allow plaintiffs to recover in the rare case that a patient's medical information is made known to the general public, probably

---

157. The first theory, unreasonable intrusion upon the seclusion of another, is not applicable to the problems set forth in this Note because most health privacy issues arise because of improper *disclosures*, not because of affirmative acts of intrusion into someone's medical records.

158. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

159. *See, e.g.*, Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1442 (1982) ("Especially when information is confined to a confidential relationship, one can imagine many cases where the greatest injury results from disclosure to a single person, such as a spouse, or to a small group, such as an insurance company resisting a claim. A confidential relationship is breached if unauthorized disclosure is made to only one person not a party to the confidence, but the right of privacy does not cover such a case." (footnotes omitted)).

160. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977). This is in contrast to the meaning of the word "publication" as it is used in connection with defamation law in Section 577, "which includes any communication by the defendant to a third person." *Id.* "The rationale behind recognizing the tort of invasion of privacy is that '[t]he right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.'" Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550, 553 (Minn. 2003) (alteration in original) (quoting Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 236 (Minn. 1998).

through the media.[161] One can think of a host of medical privacy violations that, while not disclosed to the public at large, are still very harmful to the patients involved.[162]

B. Breach of Confidentiality

1. Traditional Breach of Confidentiality Doctrine

Most jurisdictions recognize a common law cause of action for breach of confidentiality when physicians improperly disclose a patient's medical records.[163] This breach of confidentiality tort differs from invasion of privacy in several important ways. Most importantly, a breach of confidentiality claim arises from a particular relationship of trust between two individuals—in this case a doctor-patient relationship.[164] The reason behind the law's protection of such relationships is quite clear: "A patient should be entitled to freely disclose his symptoms and condition to his doctor in order to receive proper treatment without fear that those facts may become public property. Only thus can the purpose of the relationship be fulfilled."[165]

Since breach of confidentiality is premised on a specific relationship of trust, liability does not depend on the degree of offensiveness or the public nature of the disclosure.[166] An unauthorized disclosure to any third party that violates the relationship of trust between doctor and patient may be actionable.

---

161. This doctrine may still be applicable in certain cases. There have been at least a few documented examples of incidents involving public disclosure of medical records that could implicate the invasion of privacy tort. *See, e.g.*, Barbara Feder Ostrov, *140 Kaiser Patients' Private Data Put Online*, SAN JOSE MERCURY NEWS, Mar. 11, 2005, at 2C ("In a troubling episode involving medical privacy in the digital age, Kaiser Permanente is notifying 140 patients that a disgruntled former employee posted confidential information about them on her Weblog."); Alissa J. Rubin, *Column One; Records No Longer for Doctors' Eyes Only; In Today's Health Care System, Outside Parties Such as Insurers and Employees Have Access to Patients' Once-Private Medical Information. Resulting Horror Stories Have Some Seeking New Rules.*, LOS ANGELES TIMES, Sept. 1, 1998, at A1 ("Medical records of Rep. Nydia M. Velazquez's bout with depression and a year-earlier suicide attempt were faxed to reporters just four weeks before the New York Democrat's first congressional election in 1992.").

162. Notice, for example, that none of the three instances of medical privacy violations referenced in the introduction of this note would fall within this cause of action, leaving these patients with no possible legal recourse. *See supra* notes 2-4 and accompanying text.

163. Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 Rutgers L.J. 617, 654 (2002).

164. Vickery, *supra* note 154, at 1451 (stating that the duty of confidentiality "arises out of broadly applicable societal norms and public policy concerning the kind of relationship at issue").

165. McCormick v. England, 494 S.E.2d 431, 436 (S.C. 1997) (quoting Hague v. Williams, 181 A.2d 345, 349 (N.J. 1962)).

166. Winn, *supra* note 158, at 657-58.

However, certain disclosures are justified and therefore do not constitute a breach of confidentiality, particularly in circumstances where public policy concerns outweigh the patient's interest of confidentiality.[167] Furthermore, unlike the violation of privacy doctrine, disclosure under breach of confidentiality does not have to be intentional, and therefore includes circumstances where the physician is simply negligent in his or her protection of the patient's medical records.[168]

2. Reanalyzing Breach of Confidentiality in Light of the Privacy Rule

The difficulty in breach of duty cases arises when courts must ascertain whether certain disclosures of information are justified despite the duty of confidentiality that the physician owes to the patient. Such determinations should not be left to the vagaries of a judicial balancing test, nor should physicians be forced to make these difficult decisions without the benefit of some set of meaningful standards to guide them. This is especially true when these standards already exist—they are found in the Privacy Rule. Courts should adopt the Privacy Rule as a set of minimum requirements that illuminate the duty that physicians owe their patients in breach of confidentiality cases.

In traditional breach of confidentiality cases, the duty of confidentiality is derived from the protected relationship between doctor and patient. Courts, however, need not rely on a traditionally recognized relationship of confidentiality to find that a duty of confidentiality exists, because in some cases a duty may be adopted from a statute.

The Restatement (Second) of Torts states that "[t]he standard of conduct of a reasonable man may be . . . adopted by the court from a legislative enactment or an administrative regulation which does not so provide."[169] The rationale behind using a statute to define a reasonable standard of care, instead of leaving this determination up to the jury, can be summarized as follows:

> [I]t would be against the very nature of the reasonably prudent and law-abiding citizen to set one's own judgment up against that of the duly constituted lawmaking body of the community. When the community has thus officially determined that certain risks are foreseeable and are reasonably to be avoided by taking a prescribed precaution, no

167. *Id.* at 659.

168. *See* Estate of Behringer v. Med. Ctr. at Princeton, 592 A.2d 1251, 1271-72 (N.J. Super. Ct. Law Div. 1991) (finding breach of confidentiality based on negligence due to the hospital's failure to take sufficient precautions to limit accessibility of patient's chart).

169. RESTATEMENT (SECOND) OF TORTS § 285(b) (1965).

> reasonable person would thereafter omit the precaution, so there is no room for jury judgment in the matter.[170]

Thus, even though the Privacy Rule does not explicitly create a duty of confidentiality for the purpose of tort liability, it may do so by implication.

The only remaining requirement is that the statute must be intended, at least in part, to protect a particular interest held by a class of persons from a particular hazard that results in the kind of harm the plaintiff has experienced.[171] This is simply to prevent statutes from being stretched so far as to create liability where the actors, conduct, or harm are beyond the statute's intended scope.[172] The Privacy Rule certainly meets this standard since it is specifically intended to prevent the unauthorized disclosure of patient medical records by covered entities. Thus, any suit brought to remedy harm that has occurred as a direct result of such disclosure would seem to be within the scope of the law as contemplated by these requirements.

It is important to note that allowing the Privacy Rule to shape the duty of confidentiality in tort cases is not the same as creating a new federal private right of action under HIPAA. Congress has clearly chosen not to do this, and no amount of legal maneuvering will alter this decision unless Congress itself revisits the issue. There is already a preexisting common law cause of action for improper disclosure of medical records by a physician under the breach of confidentiality doctrine. The Privacy Rule acts merely as a guide, clarifying the traditional common law duty. It has long been recognized that "[a] state court is 'free to look to the provisions of a federal statute for guidance in applying its longstanding common law remedies.' "[173]

3. Advantages and Criticisms of the Breach of Confidentiality Doctrine

An obvious benefit of integrating the Privacy Rule with tort law is that it provides certainty and consistency to the nebulous scope of a defendant's duty to protect the confidentiality of a patient's medical records. The standards and principles set forth by HHS in the Privacy Rule provide a rational standard of care for a factfinder with limited experience in determining the bounds of confidentiality. Furthermore,

---

170. 3 FOWLER J. HARPER ET AL., THE LAW OF TORTS § 17.6 (2d ed. 1986).

171. RESTATEMENT (SECOND) OF TORTS § 286.

172. The leading case on this matter is *Gorris v. Scott*, (1874) 9 L.R. Exch. 125 (U.K.). In that case, defendant violated a statute requiring livestock to be kept in separate pens when being transported by ship. Plaintiff sued when his livestock was washed away during a storm. The court denied plaintiff damages, holding that the statute was designed as a sanitary measure, not to protect against the loss of livestock during a storm. *Id.* at 129.

173. Winn, *supra* note 163, at 668 (quoting Hofbauer v. Nw. Nat'l Bank, 700 F.2d 1197, 1201 (8th Cir. 1983) (quoting Iconco v. Jensen Constr. Co., 622 F.2d 1291, 1296 (8th Cir. 1980))).

since the Privacy Rule sets a baseline standard for medical record protection,[174] the general public has a reasonable expectation that its medical records will be protected pursuant to these standards. By adopting this standard of care into tort law, courts will therefore be fulfilling the public's reasonable expectations of patient privacy. Furthermore, as aforementioned, by adopting a set of clear standards of confidentiality, physicians will be better able to make reasonable and informed decisions regarding when disclosure of medical records is appropriate.

One of the major criticisms this Note directed against proposals to use § 1983 or the False Claims Act to enforce the Privacy Rule regarded issue of exorbitant damages. In contrast, a breach of confidentiality action that incorporates the standards set forth in the Privacy Rule achieves the goal of providing patients with a means of redress based on HIPAA standards, while at the same time restricting damages to more reasonable amounts.

The first step in this analysis is to reiterate that breach of confidentiality is a type of tort.[175] Tort damages are determined by the extent of plaintiff's injury and aim to redress the wrong that the defendant committed. As such, tort damages are more closely tied to traditional notions of justice than False Claims Act damages, which allow unharmed plaintiffs to recover for harm that the government sustained.

The amount of damages that a successful plaintiff is entitled to in an unauthorized disclosure of medical records case is virtually the same as in an invasion of privacy case.[176] This would include harm to the plaintiff's privacy interest, mental and emotional distress (including public humiliation), and special damages.[177] Plaintiffs can recover for mental distress without having to show physical harm;[178]

---

174. The Privacy Rule sets a national minimum level of medical record protection. While states are free to enact higher levels of protection, any state laws providing for less protection are preempted by the federal Privacy Rule. Therefore, patients can reasonably expect that their records will be afforded at least as much protection as the Privacy Rule requires. *See* 45 C.F.R. § 160.203(b) (2006) (establishing that the Privacy Rule preempts a contrary state law unless the state law provides a more stringent standard).

175. *See* Vickery, *supra* note 159, at 1451 ("First, the duty of confidentiality, where it exists, generally arises out of broadly applicable societal norms and public policy concerning the kind of relationship at issue. It does not arise out of specific agreement or particularized circumstances. Moreover, the object of the law when this duty is violated is compensation for the resulting injuries, not fulfillment of expectation. . . . Therefore, liability should be grounded in tort law.").

176. *See* Doe v. Roe, 400 N.Y.S.2d 668, 679 (N.Y.Sup. Ct. 1977) (awarding compensatory damages for embarrassment, emotional distress, and actual costs incurred, totaling $20,000).

177. RESTATEMENT (SECOND) OF TORTS §652H (1977).

178. Trevino v. Sw. Bell Tel. Co., 582 S.W.2d 582, 584 (Tex. Civ. App. 1979) (holding that in an invasion of privacy case, "[d]amages for mental suffering are recoverable without the necessity of showing actual physical injury . . .").

however, courts generally require plaintiffs to prove a high level of mental anguish in order to recover damages.[179] Plaintiffs are also entitled to recover for any pecuniary harm that was suffered as a result of the privacy violation.[180] Thus, plaintiffs would be able to recover damages for lost future earnings in situations where disclosure of medical records led to a loss of employment.

Additionally, tort law's theory of damages will limit the number of successful cases that can be brought against health care providers. Not every Privacy Rule violation will result in a successful tort suit; to prevail, plaintiffs must also demonstrate a substantial level of harm as a direct result of this violation. Thus, health care providers will not be over-burdened with litigation, while justice will not be categorically denied to plaintiffs who have been seriously harmed by the unauthorized disclosure of their medical records.

Two criticisms that may be leveled against breach of confidentiality in the medical privacy context are (1) that it does not address the issue of medical record disclosures by downstream business entities, and (2) that it may be pre-empted by ERISA. This Note posits that these potential problems can be solved, and that the breach of confidentiality doctrine will remain an effective remedy for victims of medical privacy violations.

While the traditional breach of confidentiality action provides a remedy in the case of disclosure by a physician, it does not apply to disclosures made by downstream users. Since no protected relationship of trust exists between the patient and these downstream business entities, disclosure to a third party would not be considered a breach of confidentiality. [181] So, when the disclosing party is not a physician, but rather some other covered entity, such as a hospital or an insurance company, patients may be left without a feasible remedy.

However, the Privacy Rule provides a possible solution to this gap in the common law. Under the Privacy Rule, covered entities are

---

179. *See id.* (noting that mental anguish is "more than mere disappointment, anger, resentment, or embarrassment, although it may include all of these. It includes a mental sensation of pain resulting from such painful emotions as grief, severe disappointment, indignation, wounded pride, shame, despair and/or public humiliation").

180. *See* RESTATEMENT (SECOND) OF TORTS §652H cmt. d (1977) (stating that "plaintiff may also recover for any special damage that he can prove, of which the invasion of privacy has been the legal cause").

181. While fiduciary duties are generally understood to exist in a professional context, particularly in regards to physician-patient relationships, courts are more reluctant to recognize a fiduciary duty in general business transactions. *See, e.g.*, Flights Concepts Ltd. P'ship v. Boeing Co., 819 F. Supp. 1535, 1545 (D. Kan. 1993) ("Fiduciary obligations should be extended reluctantly to commercial or business transactions."); Collins v. Nelson, 75 P.2d 570, 574 (Wash. 1938) (holding that, in order to establish a fiduciary duty, there must be something like "a business agency, a professional relationship, or a family tie").

allowed to release medical records to business associates, but are required to enter a contract with those entities to "obtain[] satisfactory assurance that the business associate will appropriately safeguard the information."[182] Professor Winn argues that this provision essentially transfers the confidentiality requirements imposed on the health care provider directly to the contracting entity.[183] Third parties were traditionally required to keep medical records confidential under the theory that they impliedly "assumed" the duty of confidentiality that the physician owed to the patient.[184] Since the third party must now expressly assume this duty under contract, it is even easier to hold these downstream business entities to the same duty of confidentiality that physicians are held to.[185] Furthermore, Winn argues that the contract between physician and business entity creates an agency relationship.[186] He suggests that plaintiffs could sue the downstream entity under a breach of confidentiality theory since, as the physician's agent, the business entity owes the same duties to the plaintiff as the physician did originally.[187] Thus, it appears likely that private parties will be able to bring tort actions against business entities that improperly disclose their medical records in much the same way as they could bring such a suit against their health care providers.

V. CONCLUSION

Medical records contain highly personal information that, if inappropriately disclosed, can have devastating effects on patients and their families. These instances of disclosure add to patient mistrust and privacy protective behaviors, which have a negative impact on the healthcare system as a whole. Congress enacted HIPAA in order to create a uniform minimum standard for the protection of medical records and to provide federal oversight to this issue. Although the statute allows the HHS Secretary to impose civil and criminal sanctions on those who blatantly ignore the Privacy Rule regulations, this type of enforcement only deters future violations—it does nothing to compensate those patients who have suffered real and direct harm as a result of such unauthorized disclosures.

Patients must have some means of redress against individuals or entities that violate the Privacy Rule. However, this action must be

182. 45 C.F.R. § 164.502(e)(1)(i) (2006).
183. Winn, *supra* note 163, at 673-74.
184. *Id.* at 673.
185. *Id.* at 673-74.
186. *Id.* at 674.
187. *Id.*

balanced against the need for health care providers to share information about their patients in order to realize the highest level of care. Subjecting doctors and hospitals to an overwhelming flood of litigation is not an adequate solution. While it might provide a strong incentive for these actors to take every necessary step for the protection of private health information, the costs of such litigation would outweigh the potential benefits. Overly cautious doctors, who refuse to share patient information with other doctors in an effort to avoid litigation or privacy liability, will compromise health care quality. Furthermore, subjecting health care providers to unnecessary litigation would only increase the already exorbitant costs of treatment. Therefore, if courts are to recognize some right of action under HIPAA, it must be carefully limited to prevent aggressive plaintiffs from suing providers for technical, benign violations.

Absent a congressional rewriting of HIPAA to explicitly recognize a private right of action, tort law provides the most sensible solution to this problem. Although a private cause of action for a Privacy Rule violation has not been recognized up to this point, there is sufficient support for the development of such an action within the common law. Such a cause of action could be created by redefining the duty of care owed under the breach of confidentiality doctrine to reflect the new standards contained in the Privacy Rule. This will allow legitimate plaintiffs to recover for actual harm that has resulted from a breach of duty established by the Privacy Rule, while simultaneously protecting health care providers from frivolous litigation and exorbitant damage awards. Incorporating the Privacy Rule into the common law duty of care will allow courts to remedy to the problem of administrative under-enforcement of the Privacy Rule.

Joshua D.W. Collins[*]

* Candidate, Doctor of Jurisprudence, Vanderbilt University Law School, May 2007. I would like to thank Professor James Blumstein for his insight and guidance throughout this process. Thanks also to all the *Law Review* members who invested their own time and effort into improving the substance and structure of this Note. Finally, thanks to my wife, Heidi, for her support and encouragement throughout my law school adventure.

***