

NOTES

GIVING HIPAA ENFORCEMENT ROOM TO GROW: WHY THERE SHOULD NOT (YET) BE A PRIVATE CAUSE OF ACTION

*Jack Brill**

INTRODUCTION

On September 21, 2007, actor George Clooney and his girlfriend Sarah Larson were injured in a motorcycle accident and taken for treatment to Palisades Medical Center in North Bergen, New Jersey.¹ During Clooney's hospital stay, several curious nurses and staff members pried into his medical records for no apparent medical reason.² In doing so, the nurses and staff members violated the Health Insurance Portability and Accountability Act (HIPAA) of 1996,³ which, in part, regulates the use of private health information.⁴ The hospital conducted an internal investigation into the matter and ultimately suspended twenty-seven nurses and staff members for one month without pay.⁵ Upon learning of the hospital's disciplinary action, Clooney remarked, "While I very much believe in a patient's right to privacy, I would hope that this could be settled without suspending medical workers."⁶

* Candidate for Juris Doctor, Notre Dame Law School, 2009; B.A., American Studies, University of Notre Dame, 2006.

1 See Bruce Lambert & Nate Schweber, *Hospital Workers Suspended for Peeking at Clooney's Files*, N.Y. TIMES, Oct. 10, 2007, at B3.

2 See *id.*

3 Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, 42 U.S.C. (2000)).

4 Specifically, the hospital workers allegedly violated HIPAA's "Security Rule," 45 C.F.R. § 164.502(a) (2007), which will be discussed in further detail *infra* Part I.B.

5 See Lambert & Schweber, *supra* note 1.

6 *Id.* (internal quotation marks omitted). Clooney did not issue a formal HIPAA complaint about the illicit prying into his medical records. *Id.*

Clooney's reaction aptly captures the tension between, on the one hand, protecting patients' privacy rights, and on the other, not overly burdening the health care system. Clooney's case involved relatively harmless curiosity over the medical records of an A-list star, but now the hospital will be short by twenty-seven workers—a consequence that will inevitably affect the hospital's ill patients. Although the invasion of Clooney's privacy did not cause him any actual damages, in many instances the illicit use of private health care information can have horrific consequences.⁷ Moreover, one can imagine situations in which the divulgence of private health information can result in extraordinary psychological hardship.⁸ Yet even when a patient suffers a severe privacy violation resulting in actual damages, HIPAA provides no private cause of action or individual remedy. Instead, the Department of Health and Human Services (HHS) oversees enforcement. Although HHS has the ability, upon finding a violation, to issue a civil fine or to turn a case over to the Department of Justice for criminal prosecution, in nearly every case HHS works informally with health care organizations⁹ to achieve compliance without implementing any sanctions.¹⁰

The potential for patients to be harmed by a HIPAA violation without having any legal recourse has led several critics to call for improvements in HIPAA enforcement. Among the commentators seeking reform are Professors Sharona Hoffman and Andy Podgurski, who have argued that a private cause of action for a HIPAA violation is necessary in order to do justice to aggrieved patients.¹¹ Specifically, Professors Hoffman and Podgurski contend that the threat of expensive and well-publicized litigation will deter HIPAA violations and result in quicker resolutions of cases as compared to administrative adjudications by agencies with limited resources.¹² To this end, Professors Hoffman and Podgurski recommend that Congress amend the HIPAA statute to create a private right of action.¹³

Professors Hoffman and Podgurski's support for a private action is compelling, but their solution may not be ideal, especially in light of

7 See *infra* notes 149–53 and accompanying text.

8 See, e.g., *infra* note 141.

9 The Privacy and Security Rules only affect specific types of health organizations. See *infra* note 19.

10 See *infra* Part I.C.

11 See Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 354–59 (2007).

12 See *id.* at 356.

13 See *id.* at 383.

recent developments to the HIPAA legal framework. This Note therefore has two chief purposes: (1) to comment on recent changes in HIPAA enforcement, guidance, and litigation; and (2) to determine, in light of those recent developments, whether affording aggrieved patients a private cause of action strikes an adequate balance between patients' privacy rights and the welfare of the health care system. To advance these aims, Part I of this Note begins by describing the HIPAA Privacy Rule, the Security Rule, and the enforcement process. Part II details recent changes to this legal framework, considering data on the current enforcement process and two recent cases in which plaintiffs sued in state courts and used HIPAA compliance as a negligence standard for common law tort claims. Finally, Part III outlines, but ultimately rejects, the argument advanced by Professors Hoffman and Podgurski on why there should be a private cause of action. This Note concludes that the costs of a private cause of action currently outweigh the benefits, and that with time, HIPAA compliance and enforcement are likely to increase even without that measure.

I. OVERVIEW OF THE HIPAA LEGAL FRAMEWORK

On August 21, 1996, Congress enacted the Health Insurance Portability and Accountability Act, known as HIPAA.¹⁴ The purpose of HIPAA was in part to develop standards for the electronic transmission of health information.¹⁵ To help attain this objective, Congress instructed HHS to create standards¹⁶ designed to ensure the privacy of individually identifiable health information.¹⁷ In late 2000, HHS formulated what became known as the HIPAA Privacy Rule,¹⁸ which articulated mandatory standards for covered entities holding personal

14 Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, 42 U.S.C. (2000)).

15 See 42 U.S.C. § 1320d note (2000) ("It is the purpose of this subtitle to improve . . . the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.").

16 See *id.* § 1320d-2 note. The standards were required to address: "(1) The rights that an individual who is a subject of individually identifiable health information should have. (2) The procedures that should be established for the exercise of such rights. (3) The uses and disclosures of such information that should be authorized or required." *Id.* § 1320d-2 note.

17 See *infra* note 24.

18 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164 (2007)).

health information.¹⁹ The HIPAA Security Rule, which specifically pertains to electronically stored health information, became effective in 2005.²⁰ HHS is also charged with enforcing the Privacy and Security Rules through a complaint process whereby patients inform HHS of perceived violations.²¹

The Privacy Rule, the Security Rule, and the resulting complaint process represent three of the most significant aspects of HIPAA's legal framework. While the Privacy and Security Rules aim to ensure the confidentiality of private health information, they are quite complex and leave covered entities with significant discretion in the implementation of the Rules. The complaint process is designed, in part, to place a check on the covered entities' discretion and to help clarify ambiguities in the Privacy and Security Rules.

A. *The HIPAA Privacy Rule*

The essential function of the HIPAA Privacy Rule²² is to permit legitimate uses of personal health information while simultaneously ensuring the privacy of that information.²³ The Rule governs the use of a patient's individually identifiable health information, which is referred to as "protected health information" (PHI).²⁴

19 HIPAA only covers health care providers, health care clearing houses, and health plans ("covered entities"). See 45 C.F.R. § 160.103(3) (2007). Many have criticized HIPAA's limited scope and argue that HIPAA should address the trafficking of private health information by entities outside of the health industry, such as marketers, employers, and lenders. See, e.g., Hoffman & Podgurski, *supra* note 11, at 344–47. I agree that HIPAA's scope should be expanded because if HIPAA is designed, at least in part, to protect patients' privacy rights, then there seems to be no good reason why some entities are not obligated to comply.

20 45 C.F.R. §§ 164.302–318 (2007).

21 See *id.* § 160.306(a).

22 For a detailed and in-depth description of the Privacy Rule's requirements, see OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE (2003) [hereinafter PRIVACY RULE SUMMARY], available at <http://www.hhs.gov/ocr/privacysummary.pdf>.

23 See *id.* at 1. (The Privacy Rule seeks to "strike[] a balance that permits important uses of [health] information, while protecting the privacy of people who seek care and healing.").

24 45 C.F.R. § 160.103 ("Health information means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.").

According to this Rule, covered entities must disclose PHI to a patient if the patient requests it, and to HHS when HHS is investigating a compliance inquiry or reviewing a complaint.²⁵ Covered entities may use or disclose PHI to the patient without the patient's request²⁶ in order to treat the patient,²⁷ to perform health care operations,²⁸ to obtain payment for services,²⁹ and for other limited purposes, such as in the event of an emergency³⁰ or for public health concerns.³¹ When

25 *See id.* § 164.502(a)(2).

26 *See id.* § 164.502(a)(1)(i).

27 *See id.* § 164.502(a)(1)(ii); *see also id.* § 164.501 (defining "treatment" as "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another").

28 *See id.* § 164.502(a)(1)(ii); *see also id.* § 164.501 (defining "health care operations" as "any of the following activities of the covered entity to the extent that the activities are related to covered functions: (1) Conducting quality assessment and improvement activities . . . (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training . . . (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits . . . (4) Conducting or arranging for medical review, legal services, and auditing functions . . . (5) Business planning and development . . . and (6) Business management and general administrative activities of the entity").

29 *See id.* § 164.502(a)(1)(ii).

30 *See id.* § 164.510(b).

31 *See id.* In addition, the Privacy Rule regulates how covered entities may disclose information to other entities that provide services, such as an administrator that assists with claims processing. The Rule refers to these entities as "business associates" of the covered entity. A "business associate" is someone who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individu-

a covered entity uses or discloses PHI, it must make reasonable efforts to limit the exposure of the PHI to the “minimum necessary.”³²

By contrast, when a covered entity uses or discloses PHI without a patient’s permission in a way falling outside the aforementioned standards, the entity commits a HIPAA violation. For example, a worker violates the rule if she looks at a patient’s PHI for any reason unrelated to the worker’s care for the patient, such as curiosity.³³ It is also a violation of HIPAA for a worker to discuss PHI in a public area, such as an elevator, cafeteria, or waiting room without a reason to do so.³⁴ Finally, it is impermissible to discuss a patient’s PHI with other staff members who are not involved with the patient’s care.³⁵

HIPAA violations, however, are not just limited to the use or disclosure of PHI—they also result when a covered entity fails to abide by certain procedural requirements mandated by the Privacy Rule. Every covered entity must have “appropriate” administrative, technical, and physical safeguards designed to ensure the privacy of PHI.³⁶ Unfortunately, the Privacy Rule fails to provide much guidance³⁷ as to what constitutes “appropriate” safeguards—it says only that a covered entity must “reasonably” safeguard PHI from illegitimate uses.³⁸ Moreover, every covered entity must implement policies and procedures pertaining to the protection of PHI that are “reasonably” designed according to a covered entity’s size and use of PHI.³⁹

ally identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

Id. § 160.103. The Privacy Rule mandates that provisions regarding the use of health information be put in the contract between the covered entity and the business associate. *See id.* § 164.504(e).

32 *Id.* § 164.502(b). The “minimum necessary” standard does not apply to the disclosure of PHI for treatment purposes, to the patient, to HHS, or if required by law. *See id.*

33 *See id.* § 164.502.

34 *See id.*

35 This is not to say that a physician, for instance, cannot discuss a patient’s symptoms and history with another physician, for such a conversation may be relevant to a patient’s care. *See id.* § 160.103.

36 *See id.* § 164.530(c)(1).

37 The lack of guidance has led covered entities to complain that the HIPAA Privacy Rule is “complicated [and] cumbersome . . . to follow.” DANIEL J. SOLOVE, *THE DIGITAL PERSON* 70 (2004).

38 § 164.530(c)(2)(i).

39 *See id.* § 164.530(i)(1) (stating that covered entities may “tak[e] into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance”). Thus, the procedures

Despite its vague description of “appropriate” safeguards, the Privacy Rule contains several concrete requirements for covered entities to ensure protection of PHI. Every covered entity must have a written policy designed to protect PHI.⁴⁰ Each covered entity must then designate a privacy official to implement procedures⁴¹ and train all members of its workforce regarding those procedures.⁴² If a covered entity discovers that an employee has violated the privacy policies and procedures, it must discipline the employee⁴³ and attempt to mitigate any potential harm that may result.⁴⁴

B. *The HIPAA Security Rule*

While the HIPAA Privacy Rule pertains to all forms of PHI, the HIPAA Security Rule⁴⁵ governs the use and disclosure of Electronic Protected Health Information (EPHI).⁴⁶ The Privacy Rule and Security Rule overlap in the sense that they both apply only to covered entities⁴⁷ and they both afford privacy protections for PHI. Their essential difference lies in coverage: the Security Rule’s scope is more limited than that of the Privacy Rule⁴⁸ because the Security Rule

implemented by a small doctor’s office might not have to be as intricate as those of a large hospital.

According to HHS, the Privacy Rule is “intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment” because “[w]hat is appropriate for a particular covered entity will depend on the nature of the covered entity’s business, as well as the covered entity’s size and resources.” PRIVACY RULE SUMMARY, *supra* note 22, at 14.

40 See 45 C.F.R. § 164.530(j)(1)(i).

41 See *id.* § 164.530(a)(1)(i).

42 See *id.* § 164.530(b)(1). The covered entity must individualize the training to the extent that each member of the workforce will be able to utilize PHI only “as necessary and appropriate . . . to carry out their function within the covered entity.” *Id.*

43 See *id.* § 164.530(e)(1). This section explains Palisades Medical Center’s disciplinary actions against the hospital workers who looked at George Clooney’s medical records. See *supra* notes 5–7 and accompanying text.

44 See 45 C.F.R. § 164.530(f).

45 *Id.* §§ 164.302–.318. For a more detailed and in-depth description of the Security Rule’s requirements, see U.S. DEP’T OF HEALTH & HUMAN SERVS., HIPAA SECURITY GUIDANCE (2006) [hereinafter SECURITY GUIDANCE], available at <http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf>.

46 See 45 C.F.R. § 164.302.

47 Covered entities are those which fall under the scope of HIPAA—health plans, health care clearing houses, and health care providers. See *supra* note 19.

48 Final Rule, Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).

promulgates separate measures that covered entities must take to ensure the security of EPHI. HHS formulated the Security Rule with the recognition that covered entities vary in terms of size and resources, and thus precautions that might be appropriate for one covered entity to protect EPHI might be insufficient for another covered entity.⁴⁹ Accordingly, the Security Rule gives covered entities the discretion to tailor safeguards and procedures to fit their own needs.⁵⁰

The Security Rule has four general requirements. Covered entities must:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.⁵¹

There are three categories of safeguards to support these general requirements: administrative safeguards,⁵² physical safeguards,⁵³ and technical safeguards.⁵⁴ HHS has formulated standards and implementation procedures for each safeguard to be met.⁵⁵ Each covered

49 *See id.* (“[T]he entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution . . . that would be useable by all covered entities.”).

50 In drafting the Security Rule, HHS sought to adhere to the concept of “technological neutrality” so that covered entities may “select appropriate technology solutions and to adopt new technology over time.” *Id.* Accordingly, the Security Rule was written using “standards in terms that are as generic as possible [so that they] may be met through various approaches or technologies.” *Id.* at 8336.

51 45 C.F.R. § 164.306(a).

52 *See id.* § 164.308.

53 *See id.* § 164.310.

54 *See id.* § 164.312.

55 Every covered entity must adhere to the standards, but the implementation procedures are divided into two categories, “required” and “addressable.” *Id.* § 164.306(d)(1). “Required” implementation procedures are mandatory, *see id.* § 164.306(d)(2), whereas “addressable” implementation procedures require the entity to determine whether the implementation specification is a reasonable and appropriate safeguard given the entity’s environment, *see id.* § 164.306(d)(3)(i). If so, the entity must implement it. *See id.* § 164.306(d)(3)(ii). If the entity determines that the implementation procedure is not reasonable, then the entity must document that it has drawn this conclusion, *see id.* § 164.306(d)(3)(ii)(B)(1), and implement a similar procedure if “reasonable and appropriate,” *id.* § 164.306(d)(3)(ii)(B)(2).

entity has a perpetual duty to renew and modify its security provisions to ensure reasonable protection of EPHI.⁵⁶

1. Administrative Safeguards

The administrative safeguards section of the HIPAA Security Rule is quite verbose and comprises over half of the Security Rule's requirements.⁵⁷ These safeguards include the implementation of a plan designed to "prevent, detect, contain, and correct" security violations.⁵⁸ In formulating the plan, covered entities must engage in a risk analysis regarding the potential vulnerabilities of their EPHI storage,⁵⁹ and they must implement policies to reduce such risks.⁶⁰ Covered entities must also designate one individual to be responsible for the development and implementation of the security plan,⁶¹ and, like the Privacy Rule, the Security Rule requires covered entities to punish employees who fail to abide by the covered entity's security procedures.⁶² Other administrative safeguards include the development of a workforce security plan designed to ensure that only those workers who need to access EPHI can do so,⁶³ the development of policies and procedures for the authorization of access to EPHI,⁶⁴ the implementation of a security training program for workers,⁶⁵ and the development of a procedure designed to respond to security incidents and threats.⁶⁶

56 *See id.* § 164.306(e).

57 For a detailed overview of the administrative safeguards section of the Security Rule, see CTRS. FOR MEDICARE & MEDICAID SERVS., U.S. DEP'T OF HEALTH & HUMAN SERVS., SECURITY STANDARDS: ADMINISTRATIVE SAFEGUARDS (2007) [hereinafter ADMINISTRATIVE SAFEGUARDS], *available at* <http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsAdministrativeSafeguards.pdf>.

58 45 C.F.R. § 164.308(a)(1)(i).

59 *See id.* § 164.308(a)(1)(ii)(A). In evaluating the vulnerabilities of EPHI, HHS recommends that covered entities consider how EPHI is created, received, maintained, and transmitted. *See* ADMINISTRATIVE SAFEGUARDS, *supra* note 57, at 4. For other factors that covered entities may wish to consider, see *id.*

60 45 C.F.R. § 164.308(a)(1)(ii)(B).

61 *See id.* § 164.308(a)(2).

62 *See id.* § 164.308(a)(1)(ii)(C).

63 *See id.* § 164.308(a)(3)(i). HHS suggests developing and implementing a two-factor authentication for employees accessing EPHI from a remote location by requiring the employee to answer a security question (such as "favorite pet's name") in addition to a username and password. *See* SECURITY GUIDANCE, *supra* note 45, at 4.

64 *See* 45 C.F.R. § 164.308(a)(4).

65 *See id.* § 164.308(a)(5).

66 *See id.* § 164.308(a)(6).

2. Physical Safeguards

The physical safeguards section of the Security Rule has four standards which pertain to facility access, workstation⁶⁷ use, workstation security, and device and media controls.⁶⁸ Covered entities must implement policies to limit physical access to EPHI and its storage facility, while at the same time ensuring that authorized personnel have access to it.⁶⁹ Covered entities must also create policies that specify the appropriate use of workstations with access to EPHI,⁷⁰ and implement physical safeguards that restrict access to such workstations.⁷¹ Finally, policies and procedures must be put in place to govern the receipt and removal of electronics and hardware containing EPHI.⁷²

3. Technical Safeguards

The technical safeguards of the Security Rule are designed to ensure that only authorized persons have access to EPHI.⁷³ Covered entities must implement technical policies and procedures pertaining to electronic information systems that maintain EPHI in order to limit access to only those authorized persons.⁷⁴ The Security Rule mandates that covered entities assign a unique name or number to authorized users so as to track user identity;⁷⁵ there also must be a system in

67 “Workstation” is defined as “an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.” *Id.* § 164.304.

68 For a detailed overview of the physical safeguards requirements, see CTRS. FOR MEDICARE & MEDICAID SERVS., U.S. DEP’T OF HEALTH & HUMAN SERVS., SECURITY STANDARDS: PHYSICAL SAFEGUARDS (2007) [hereinafter PHYSICAL SAFEGUARDS], available at <http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsPhysicalSafeguards.pdf>.

69 See 45 C.F.R. § 164.310(a)(1). HHS recommends making sure appropriate doors are locked, restricted access signs are posted, and perhaps even the use of identification badges for authorized personnel and arranging for private security to patrol the facility. See PHYSICAL SAFEGUARDS, *supra* note 68, at 5.

70 See 45 C.F.R. § 164.310(b).

71 See *id.* § 164.310(c).

72 See *id.* § 164.310(d)(1). For instance, when disposing of hardware, HHS recommends “degaussing”—using magnets to fully erase data from a hard drive. See PHYSICAL SAFEGUARDS, *supra* note 68, at 11.

73 For a detailed overview of the technical safeguards, see CTRS. FOR MEDICARE & MEDICAID SERVS., U.S. DEP’T OF HEALTH & HUMAN SERVS., SECURITY STANDARDS: TECHNICAL SAFEGUARDS (2007) [hereinafter TECHNICAL SAFEGUARDS], available at <http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf>.

74 See 45 C.F.R. § 164.312(a)(1).

75 See *id.* § 164.312(a)(2)(i).

place whereby access to EPHI may be obtained during an emergency.⁷⁶ Covered entities must install hardware and software to record and examine activity in electronic information systems that contain EPHI,⁷⁷ and procedures must be developed to protect the integrity of EPHI—that is, to ensure that it is neither altered nor destroyed.⁷⁸ Finally, covered entities must have a procedure that ensures that the person seeking access to EPHI is indeed authorized.⁷⁹

Collectively, the Security Rule provisions function to limit the access and use of EPHI to appropriate purposes. Like the Privacy Rule, the Security Rule gives covered entities significant discretion to analyze their own uses of health information and to develop “reasonable” safeguards to ensure the privacy of such health information. Thus, the same criticism of the Privacy Rule is applicable to the Security Rule. Vague regulations create the risk that covered entities will incorporate less rigorous (and thus less expensive) standards. Moreover, there are legitimate concerns that covered entities may not even be competent to judge what constitutes reasonable or appropriate safeguards.⁸⁰ The HIPAA enforcement process, discussed next, is designed to alleviate such concerns.

C. *The HIPAA Enforcement Procedure*

If a patient believes that her privacy rights have been compromised, or if a patient believes that there is an absence of appropriate security measures within a covered entity, she may file a complaint to

76 *See id.* § 164.312(a)(2)(ii). For instance, there must be a way to access PHI if the electricity goes out or if a computer crashes. There are two other “addressable” implementation procedures—installing an “automatic log-off” program that terminates an electronic session after a certain period of time, *see id.* § 164.312(a)(2)(iii), and implementing a mechanism that encrypts and decrypts EPHI, *see id.* § 164.312(a)(2)(iv).

77 *See id.* § 164.312(b).

78 *See id.* § 164.312(c)(1). The Security Rule also requires a procedure to prevent unauthorized access to EPHI when EPHI is being transmitted over an electronic communications network. *See id.* § 164.312(e).

79 *See id.* § 164.312(d). HHS recommends the use of passwords or personal identification numbers, or perhaps even smartcards or biometrics (fingerprints, voice patterns, facial patterns, or iris patterns). *See TECHNICAL SAFEGUARDS, supra* note 73, at 9–10.

80 *See, e.g.,* Hoffman & Podgurski, *supra* note 11, at 351 (“In the context of the Security Rule, it is unrealistic to expect that every health care provider has the technical expertise and ability to determine on its own how to implement the security standards. Furthermore, some organizations could use the regulations’ vagueness as a justification for establishing minimal PHI security measures.”).

HHS.⁸¹ The Office for Civil Rights (OCR), an agency within HHS, handles complaints related to violations of the Privacy Rule,⁸² and the Centers for Medicare and Medicaid Services (CMS), another agency within HHS, handles complaints related to the Security Rule.⁸³ When a complaint alleges violations of both the Privacy Rule and the Security Rule, OCR will coordinate an investigation with CMS.⁸⁴

If, after an investigation, OCR or CMS determines that a violation has occurred, the Secretary of HHS will inform the covered entity of the noncompliance.⁸⁵ The Secretary will work informally with the covered entity to achieve compliance, which may be accomplished by the covered entity demonstrating adequate compliance or by implementing a satisfactory corrective action plan.⁸⁶ If the covered entity does not take satisfactory action to resolve the matter, then the Secretary has authority to impose civil fines on the entity.⁸⁷ Willful violations may be turned over to the Justice Department for criminal prosecution.⁸⁸

81 See 45 C.F.R. § 160.306(a). The enforcement provisions are applicable to both the Privacy Rule and the Security Rule. See *id.* § 160.300 (“This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.”). The Secretary has discretion to investigate complaints. See *id.* § 160.306(c) (“The Secretary *may* investigate complaints filed under this section.” (emphasis added)). Factors to be considered when deciding whether to pursue an investigation include whether the complaint is directed at the actions of a covered entity and whether the complaint, if true, would constitute a violation. See U.S. Dep’t of Health & Human Servs., Compliance and Enforcement: What OCR Considers During Intake & Review of a Complaint, <http://www.hhs.gov/ocr/privacy/enforcement/complaintreview.html> (last visited Apr. 8, 2008).

82 See 45 C.F.R. § 160.306(b) for the basic requirements of filing a complaint.

83 Statement of Organization, Functions, and Delegations of Authority, 68 Fed. Reg. 60,694, 60,694 (Oct. 23, 2003).

84 See U.S. Dep’t of Health & Human Servs., Compliance and Enforcement: How OCR Enforces the HIPAA Privacy Rule, <http://www.hhs.gov/ocr/privacy/enforcement/hipaarule.html> (last visited Apr. 8, 2008).

85 See 45 C.F.R. § 160.312(a). If the covered entity disagrees with the assessment of HHS, it may request a hearing before an administrative law judge. See *id.* § 160.504(a).

86 See *id.* § 160.312(a)(1).

87 See 42 U.S.C. § 1320d-5 (2000).

88 See *id.* § 1320d-6. (“A person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished”). The Department of Justice has interpreted § 1320d-6 to impose criminal liability only against covered entities and “depending on the facts of a given case, certain directors,

The HIPAA complaint process seems to alleviate some, though certainly not all, concerns about the effectiveness of the Privacy and Security Rules. Specifically, any uncertainty that a covered entity may have over its own implementation of the Privacy and Security Rule standards can be clarified if, after receiving a complaint, HHS works informally with a covered entity to develop a corrective action plan. Yet several concerns remain. For instance, the current system can only work if enough patients file complaints and if HHS has enough resources to work with covered entities to develop corrective action. Moreover, the complaint process only provides post hoc clarification to a particular covered entity, and thus does not result in universal clarification as to what might constitute a reasonable safeguard. Finally, the legal recourse of aggrieved patients is limited to filing a complaint with HHS, which critics consider unjust and inadequate. To address these perceived flaws in the HIPAA model, many commentators have suggested reforms, including the creation of a private cause of action. Yet before addressing the argument for a private cause of action,⁸⁹ it is first necessary to explore HIPAA's current state of affairs, which exists following several recent developments in the HIPAA framework.

II. RECENT DEVELOPMENTS IN HIPAA ENFORCEMENT, GUIDANCE, AND LITIGATION

The HIPAA legal framework has recently undergone two important changes in terms of enforcement, guidance, and litigation. First, OCR and CMS have begun to release statistics on HIPAA enforcement, and they have also provided clarification of several confusing aspects of the Privacy and Security Rules. A second major development involves two recent state court decisions that have incorporated HIPAA as a standard of negligence for common law tort claims. These developments are significant because they indicate that HHS is taking a proactive role in working with covered entities to achieve compliance and that aggrieved patients might be able to use a violation of the Privacy and Security Rules to obtain money damages.

officers, and employees of these entities." Memorandum Opinion for the General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6 (June 1, 2005), http://www.usdoj.gov/olc/hipaa_final.htm. Thus, other persons or organizations that obtain PHI will not be prosecuted under the HIPAA criminal provision. *See id.*

89 *See infra* Part III.A.

A. *Improved HIPAA Enforcement and Guidance*

Beginning in April 2007, perhaps to stave off criticism for what many perceived as a poor enforcement record,⁹⁰ OCR began putting monthly updates on enforcement of Privacy Rule violations on its website.⁹¹ As of December 31, 2007, OCR had received 32,487 Privacy Rule complaints, of which 25,743 (79%) have been resolved.⁹² Of those resolved complaints, OCR had initiated formal investigations in 8199 cases, and corrective action was obtained in 5509 of those investigations.⁹³ In the rest of the investigations, OCR determined that no violation had occurred.⁹⁴ The statistics also indicate that since 2003, when the Privacy Rule first took effect, OCR has steadily increased the number of investigations that it has engaged in each year.⁹⁵ The number of corrective actions has also increased on a yearly basis.⁹⁶ These figures suggest that since the Privacy Rule's inception, OCR has become more efficient at both investigating complaints and working with covered entities to ensure compliance.

OCR's new website also helps covered entities learn from the violations of other covered entities. This website contains a list of actual instances of HIPAA violations and the ensuing corrective actions that covered entities took to avoid future violations.⁹⁷ There is also a "What's New" section on the OCR website, which provides frequent

90 See *Keep Your Hands Off My PHI: Security Complaints Mimic Privacy*, REPORT ON PATIENT PRIVACY, July 2007, at 4, 5 [hereinafter *Complaints Mimic Privacy*] (reporting that OCR reformatted its website in response to criticism of its enforcement figures).

91 See Press Release, Office for Civil Rights, U.S. Dep't of Health & Human Servs., HHS Launches New Web Site on HIPAA Privacy Compliance and Enforcement (Apr. 20, 2007), available at <http://www.hhs.gov/ocr/privacy/enforcement/announcement.html> ("To coincide with the fourth anniversary of the enforcement of the HIPAA Privacy Rule, the Department of Health and Human Services (HHS) announced today the launch of an enhanced Web site that will make it easier for consumers, health care providers and others to get information about how the Department enforces health information privacy rights and standards.").

92 See Office for Civil Rights, U.S. Dep't of Health & Human Servs., Compliance and Enforcement: Numbers at a Glance, <http://www.hhs.gov/ocr/privacy/enforcement/numbersglance1207.html> (last visited Apr. 8, 2008). OCR provides monthly updates on the number of complaints that they receive. See *id.*

93 See *id.*

94 See *id.*

95 See *id.* (reporting 339 investigations in 2003; 1392 in 2004; 1803 in 2005; and 2466 in 2006).

96 See *id.* (reporting 260 corrective actions in 2003; 1033 in 2004; 1161 in 2005; and 1571 in 2006).

97 See Office for Civil Rights, U.S. Dep't of Health & Human Servs., Compliance and Enforcement: All Case Examples, <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html> (last visited Apr. 8, 2008).

updates on privacy issues pertinent to HIPAA and HIPAA enforcement.⁹⁸ Moreover, a “Frequently Asked Questions” webpage is available,⁹⁹ as are HIPAA educational materials which contain guides to Privacy Rule compliance, such as a sample business associate contract that comports with the Privacy Rule, a guide for drafting written notices of a covered entity’s privacy policy, and other materials.¹⁰⁰

During the summer of 2007, CMS also made Security Rule complaint data available online.¹⁰¹ As of December 31, 2007, CMS had received 1043 Security Rule complaints.¹⁰² Of those complaints, 892 (86%) have been closed after corrective action in 49 cases.¹⁰³ Like OCR, CMS also provides significant guidance as to how to achieve compliance with the Security Rule.¹⁰⁴ CMS even published a report on how covered entities can incorporate plans to reduce the risk of theft when remote access to EPHI is necessary.¹⁰⁵ This report was prepared in response to recent stolen laptops containing EPHI.¹⁰⁶

The fairly high percentage of complaints resolved by OCR and CMS, combined with the agencies’ efforts to inform covered entities how to comply with HIPAA’s Privacy and Security Rules, suggests that HHS is actively engaged in HIPAA enforcement and compliance. In addition to such efforts, there are other positive signs that HIPAA enforcement may be on the rise. For instance, in April 2007, the Secretary of HHS delegated subpoena authority to OCR, thus allowing

98 See Office for Civil Rights, U.S. Dep’t of Health & Human Servs., Current and Previously Posted What’s New Items, <http://www.hhs.gov/ocr/whatsnew.html> (last visited Apr. 8, 2008).

99 See U.S. Dep’t of Health & Human Servs., About the Privacy Rule FAQs, <http://www.hhs.gov/hipaafaq/about/index.html> (last visited Apr. 8, 2008).

100 See Office for Civil Rights, U.S. Dep’t of Health & Human Servs., Medical Privacy—National Standards to Protect the Privacy of Personal Health Information, <http://www.hhs.gov/ocr/hipaa/assist.html> (last visited Apr. 8, 2008).

101 See *Complaints Mimic Privacy*, *supra* note 90, at 5 (“CMS’s decision to begin posting information about security complaints was based on OCR’s move in this direction. OCR had been enforcing the rule for three years, however, before it began the Website postings . . .”).

102 See Ctr. for Medicare & Medicaid Servs., U.S. Dep’t of Health & Human Servs., CMS Enforcement Statistics Report: Open and Closed Cases by Type as of December 31, 2007, <http://www.cms.hhs.gov/Enforcement/Downloads/EnforcementStatistics-December2007.pdf> (last visited Apr. 8, 2008).

103 See *id.*

104 See, e.g., ADMINISTRATIVE SAFEGUARDS, *supra* note 57; PHYSICAL SAFEGUARDS, *supra* note 68; SECURITY GUIDANCE, *supra* note 45; TECHNICAL SAFEGUARDS, *supra* note 73.

105 See SECURITY GUIDANCE, *supra* note 45.

106 See *id.*; see also *infra* notes 149–53 and accompanying text (discussing news stories reporting stolen laptops).

OCR to conduct more thorough investigations.¹⁰⁷ Additionally, HHS recently administered its first ever audit of a hospital in which HHS requested information pertaining to the hospital's electronic security policies and procedures.¹⁰⁸ These recent developments have led one law firm to issue a newsletter entitled *Covered Entities Be Warned: A New Era of HIPAA Enforcement Is Upon Us*.¹⁰⁹ The ultimate effect of HHS's attempts to increase HIPAA compliance remains uncertain. Yet there can be no doubt that these recent efforts are at least steps in the right direction.

B. HIPAA Violations as the Standard of Negligence in State Court

The text of HIPAA provides no private right of action, and federal courts have consistently held that no federal subject matter jurisdiction exists for claims alleging a HIPAA violation because a private right of action cannot be implied.¹¹⁰ In 2006, however, there were

107 Delegations of Authority, 72 Fed. Reg. 18,999, 18,999 (Apr. 16, 2007) (the Secretary may "requir[e] the attendance and testimony of witnesses and the production of any evidence that relates to any matter under investigation or compliance review for failure to comply with [HIPAA] standards and requirements related to the privacy of individually identifiable health information").

108 See *Audit Raises Concerns of Data Security Requirements*, HIPAA REGULATORY ALERT, Aug. 2007, at 3, 3 [hereinafter *Audit Raises Concerns*] (reporting that the audit is "raising concerns in the information technology industry that there may be more HHS enforcement actions relating to HIPAA data security requirements"); see also Augustine S. Weekley, *HIPAA in Private Tort Litigation*, LEGAL UPDATE (Holland & Knight), Oct. 2007, http://www.lorman.com/newsletters/article.php?article_id=830&newsletter_id=182&category_id=8&topic=LIT ("[O]ther hospitals are certainly taking notice, and many are upgrading their security systems or taking other data protection measures."). But see *Audit Raises Concerns*, *supra*, at 5 (reporting that one industry analyst "doubts the audit will lead many other organizations to step up efforts to comply with security requirements"). It should be noted that CMS did not conduct the audit—it was conducted by HHS's Office of the Inspector General. See *id.*

109 *Covered Entities Be Warned: A New Era of HIPAA Enforcement Is Upon Us*, HEALTH CARE ADVISORY (Alston & Bird, LLP), May 1, 2007, at 1.

110 See, e.g., *Acara v. Banks*, 470 F.3d 569, 571–72 (5th Cir. 2006) ("Every district court that has considered this issue is in agreement that the statute does not support a private right of action. . . . We hold there is no private cause of action under HIPAA . . ."); *O'Donnell v. Blue Cross Blue Shield of Wyo.*, 173 F. Supp. 2d 1176, 1180 (D. Wyo. 2001) ("[C]ongress did not intend to create an implied private cause of action."). Given the Supreme Court's decision in *Alexander v. Sandoval*, 532 U.S. 275 (2001), it is highly unlikely that any federal court would imply a private cause of action in HIPAA. Under *Sandoval*, to determine whether a federal statute provides a private remedy, the only relevant inquiry is whether Congress "displays an intent" to create a private cause of action and private remedy. See *id.* at 286–87. The Court reasoned that "[t]he express provision of one method of enforcing a substantive rule suggests that Congress intended to preclude others." *Id.* at 290. Since HIPAA does

two cases in which a plaintiff in state court was able to incorporate HIPAA as a standard of care in a common law tort claim.¹¹¹ These cases, *Acosta v. Byrum*¹¹² and *Sorensen v. Barbuto*,¹¹³ sparked considerable discussion in recent legal literature,¹¹⁴ leading one commentator to assert: “Thus begins what is likely to be a line of civil cases using HIPAA as a standard for the measurement of the duty to maintain health care privacy.”¹¹⁵

Acosta involved a North Carolina patient’s claim against a doctor for negligent infliction of emotional distress.¹¹⁶ The plaintiff, Heather Acosta, was a psychiatric patient at Psychiatric Associates, which was owned by defendant Dr. David Faber.¹¹⁷ During Acosta’s time as a patient, defendant Robin Byrum, the office manager of Psychiatric Associates, developed a personal animus towards Acosta.¹¹⁸ The basis for the lawsuit against Faber was Acosta’s allegation that Faber improperly permitted Byrum to use his medical access number to acquire Acosta’s medical records, including her confidential psychiatric information.¹¹⁹ Byrum in turn disclosed this information to

not explicitly provide for a private cause of action, and instead provides for administrative enforcement, a private cause of action is not, and should not be, read into the statute.

111 As Professors Hoffman and Podgurski explain, it is difficult to establish common law tort claims for a HIPAA violation. The two most promising theories, the tort of public disclosure of private facts and the tort of breach of confidentiality, will not be applicable in many situations. See Hoffman & Podgurski, *supra* note 11, at 358–59. The tort of public disclosure of private facts will usually fail because it requires widespread public dissemination, and the typical HIPAA violation involves the disclosure of health information to specific parties. See *id.*; see also RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977) (“[I]t is not an invasion of the right of privacy . . . to communicate a fact concerning the plaintiff’s private life to a single person or even to a small group of persons.”). The tort of breach of confidentiality similarly will fail in many instances because it requires a direct relationship between the perpetrator and the plaintiff. See Hoffman & Podgurski, *supra* note 11, at 358; see also Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 512 (1995) (“The rule of confidentiality does not work nearly as well in a modern information society [because health] data today, in an era of electronic information gathering, is based only in small part on the physician-patient relationship.”).

112 638 S.E.2d 246 (N.C. Ct. App. 2006).

113 143 P.3d 295 (Utah Ct. App. 2006), *aff’d*, 177 P.3d 614 (Utah 2008).

114 See, e.g., Reginald C. Govan, *Personnel, Investigative, and Health Records*, in 2 PRACTISING LAW INST., 36TH ANNUAL INSTITUTE ON EMPLOYMENT LAW 409, 533 (2007) (discussing *Acosta* and *Sorensen*); Weekley, *supra* note 108 (same).

115 See Weekley, *supra* note 108.

116 See *Acosta*, 638 S.E.2d at 249.

117 See *id.*

118 See *id.*

119 See *id.*

other parties without Acosta's authorization, and consequently, she suffered severe emotional distress.¹²⁰ Acosta sued Byrum for intentional infliction of emotional distress and Faber for negligent infliction of emotional distress.¹²¹ The suit against Faber was dismissed at trial for failure to state a claim, but the plaintiff filed an interlocutory appeal, which resulted in reversal.¹²²

As part of her complaint, Acosta alleged that when Faber allowed Byrum to use his access code, he negligently engaged in conduct that was in violation of HIPAA.¹²³ The North Carolina Court of Appeals held that Acosta had sufficiently pled a claim for negligent infliction of emotional distress.¹²⁴ In so holding, the court agreed with Acosta that the trial court's dismissal of the complaint on the grounds that HIPAA does not grant an individual a private cause of action was improper.¹²⁵ The court recognized that Acosta cited to HIPAA as evidence of the appropriate standard of care, a necessary element of negligence.¹²⁶ Thus, Faber was "on notice that plaintiff [would] use the rules and regulations of . . . HIPAA to establish the standard of care."¹²⁷

The second potentially important case decided in 2006 is *Sorensen*. The plaintiff, Nicholas Sorensen, was injured in an automobile accident and was subsequently treated by the defendant, Dr. John P. Barbuto.¹²⁸ Eventually, Sorensen's medical insurance prevented Sorensen from continuing to see Barbuto for treatment.¹²⁹ Yet when Sorensen filed a personal injury lawsuit against the driver of the automobile, Barbuto had an ex parte discussion pertaining to Sorensen's medical condition with the defense counsel.¹³⁰ Barbuto even

120 *See id.*

121 *See id.* In North Carolina, the negligent infliction of emotional distress tort requires that the defendant negligently engaged in conduct, that it was reasonably foreseeable that defendant's conduct would cause severe emotional distress, and that the plaintiff in fact suffered from severe emotional distress. *See id.* at 250.

122 *See id.* at 250–52.

123 *See id.* at 249.

124 *See id.* at 252.

125 *See id.* at 253.

126 *See id.*

127 *Id.* at 251. Ostensibly, Faber's actions constituted a violation of the Security Rule because he allowed an unauthorized person to access EPHI. *See supra* notes 69–75 and accompanying text.

128 *See Sorensen v. Barbuto*, 143 P.3d 295, 297–98 (Utah Ct. App. 2006), *aff'd*, 177 P.3d 614 (Utah 2008).

129 *See id.* at 298.

130 *See id.*

agreed to serve as an expert witness at the trial for the defense.¹³¹ When Sorensen found out about the *ex parte* communications, he successfully convinced the trial court to exclude Barbuto's testimony, and he ultimately prevailed in the lawsuit.¹³² Sorensen then initiated the present suit against Barbuto, alleging, among other claims, a breach of professional duty.¹³³ The trial court dismissed all the claims and Sorensen appealed.¹³⁴

The appellate court, albeit in a footnote, rejected Barbuto's argument that Sorensen was not entitled to a private cause of action for the tort of negligent breach of fiduciary duty of confidentiality.¹³⁵ The court pointed out that Sorensen did not contend that a separate private cause of action exists for the violating professional standards, but rather that "[Sorensen] asserts that the professional standards contribute to the proper standard of care, citing the Health Insurance Portability and Accountability Act."¹³⁶ Ultimately, the court reversed the trial court and held that Sorensen had stated a cause of action for a negligent breach of confidentiality.¹³⁷ In so doing, the court implied that a violation of the Privacy Rule can be used to establish the standard of care.¹³⁸

As a legal matter, the holdings of *Acosta* and *Sorensen* have intuitive appeal—HIPAA provides standards of conduct, and as such, when a doctor fails to comply with HIPAA, she may very well be negligent. But given HIPAA's complexity and the discretion that it affords covered entities, it might not be reasonable in all instances for covered entities to be expected to know how to comply with HIPAA's complicated requirements. Indeed, HHS recognized the difficulties in abiding by the Privacy and Security Rules and therefore, rather than first issuing a fine for a violation, it works with a covered entity to achieve compliance.¹³⁹ As will be discussed in further detail in Part III.B, *Acosta* and *Sorensen* illustrate the varying degrees of difficulty that judges and juries might face in determining whether a violation has even occurred. Due to practical considerations, as well as other policy

131 *See id.*

132 *See id.*

133 *See id.*

134 *See id.*

135 *See id.* at 299 n.2.

136 *Id.*

137 *See id.* at 300–01.

138 In disclosing medical information without Sorensen's consent, Barbuto may have violated the Privacy Rule's prohibition of unauthorized disclosures. *See* 45 C.F.R. § 164.502(a) (2007). Yet, as will be discussed *infra* Part III.B, there has been some disagreement as to the Privacy Rule's effect on *ex parte* communications.

139 *See* 45 C.F.R. § 160.312(a)(1).

and economic reasons, state courts should be hesitant to equate a HIPAA violation with negligence.

It is too early to determine the ultimate effect that *Acosta* and *Sorensen* will have on litigation involving HIPAA violations in state courts. Both decisions came from courts of appeals and thus not from a state's highest court.¹⁴⁰ As of April 2008, no other court had cited *Acosta* or *Sorensen* for the proposition that a violation of HIPAA may be used as the standard of negligence in a state law tort claim. Nevertheless, if other state courts adopt the notion that HIPAA can provide guidance as to the standard of care in negligence claims, then courts may see a dramatic increase in HIPAA-related litigation.

The recent changes in the HIPAA legal framework are important to the question of whether Congress should confer a federal private cause of action. If HHS is capable of enforcing the Privacy and Security Rules, as the statistics seem to indicate, then there may be no need to bring HIPAA enforcement to the private sector. Moreover, if HIPAA litigation becomes prevalent in state courts, the costs of HIPAA compliance will surely increase. A federal cause of action would further increase these compliance costs and lead to more expensive health care. The debate over a private cause of action, discussed next, must take into account the effectiveness of HIPAA enforcement and the significant costs of HIPAA compliance.

III. THE DEBATE SURROUNDING A PRIVATE CAUSE OF ACTION

Perceived ineffectiveness in HIPAA enforcement and the lack of a remedy for aggrieved patients have led several commentators and organizations to argue that patients' privacy rights would be best protected by adding the deterrent of private litigation to the HIPAA legal framework. Although the arguments supporting a private cause of action may be compelling, ultimately it is not the best solution to any deficiencies in HIPAA compliance given practical, economic, and policy considerations.

140 The Utah Supreme Court affirmed the appellate court's holding that *Sorensen* had pled a valid claim for negligent breach of the duty of confidentiality, but it did not specifically address *Sorensen*'s use of HIPAA to establish the standard of care. See *Sorensen v. Barbuto*, 177 P.3d 614, 620 (Utah 2008). The issue before the Utah Supreme Court was whether *Barbuto*'s ex parte communications with opposing counsel constituted a violation of *Barbuto*'s fiduciary duty of confidentiality. See *id.* The court's opinion, therefore, does not foreclose the use of HIPAA to establish the standard of care because the negligence issue was not before the court.

A. *The Argument in Favor of a Private Cause of Action*

There are many reasons why it is important to keep one's personal health information private. For instance, if personal health information were accessible, employers might use the information to recruit the healthiest employees, and lenders might use personal health information in deciding whether to grant a loan.¹⁴¹ One's personal health information could be even more lucrative to lenders and employers if it included information about genetic predispositions. Medical identity theft is also a huge concern that could jeopardize one's health and even lead to legitimate insurance claims being denied.¹⁴² In addition to details pertaining to a person's health, medical records also contain other information, such as names, addresses, social security numbers, and billing information, all of which can be used to steal an identity.

141 See Hoffman & Podgurski, *supra* note 11, at 334–35 (discussing reasons why the security of personal health information is important). Professors Hoffman and Podgurski hypothesize that personal health information might also be useful to educational institutions who might favor healthier students, and even potential romantic partners who do not want to get involved with unhealthy mates. *Id.*; see also Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 621 (2002) (“The disclosure of certain types of adverse health information can have a powerful, often destructive, impact on the person who is the subject of that information. Many diseases have a social stigma that no laws against discrimination can banish. Even the disclosure of some medical conditions that are not contagious and have no adverse impact on others may damage an individual's reputation with colleagues, friends, and family.”).

For those workers who take “sick days” from work when they are in fact healthy, HIPAA's Privacy Rule prevents their bosses from verifying their doctors' notes, which has led to some creative business ideas. See Johnny Johnson, *When It Comes to Missing Work What's Your Excuse?*, OKLAHOMAN, Oct. 26, 2007, at 1A (reporting on a business that sells authentic-looking doctor's notes to workers who wish to call in sick).

142 See, e.g., Adam Levin, Editorial, *A New and Growing Threat to Health: Medical Identity Theft*, STAR LEDGER (Newark, N.J.), Feb. 20, 2007, at 11 (discussing the consequences of medical identity theft). The physical and financial ramifications of medical identity theft can be astounding. For instance, if *A* steals *B*'s health information and uses that information to see a doctor under *B*'s insurance, then *B* will receive a bill and *A*'s use of the insurance will count against *B*'s quota. Even worse, it is possible that *B*'s medical records will be altered by *A*'s condition, which can lead to deadly results—for instance, *B*'s medical record might be altered to include *A*'s blood type. These situations are not all that uncommon. The *Los Angeles Times* reported that in 2003 alone, there were over 200,000 instances of medical identity fraud. See Joseph Menn, *ID Theft Infects Medical Records*, L.A. TIMES, Sept. 25, 2006, at A1. Although certainly not all medical identity fraud is stolen from covered entities, the wealth of personal health records that many covered entities maintain certainly makes them susceptible to theft.

Given the strong interest that patients have in keeping their health information private, HHS is left with an extraordinary responsibility to police the standards set forth in the Privacy and Security Rules. Yet since the enforcement process is primarily complaint driven,¹⁴³ private citizens also play a crucial role in ensuring HIPAA compliance by filing complaints. The complementary roles that HHS and patients have in enforcing the Privacy and Security Rules begs the obvious question: would the goal of keeping personal health information private be more efficiently met by changing the enforcement process to confer a private cause of action for a violation?

As of January 2008, HHS had yet to impose a civil fine on a covered entity for a HIPAA violation.¹⁴⁴ While hundreds of cases have been referred by HHS to the DOJ for criminal prosecution,¹⁴⁵ there have been only four criminal convictions for a HIPAA violation to date.¹⁴⁶ These sparse numbers have led many commentators to call for stricter enforcement of HIPAA's Privacy and Security Rules.¹⁴⁷ Others have criticized the complaint-driven enforcement process,

143 See *supra* Part I.C.

144 See E-mail from Shirlene Peterson, Program Assistant, U.S. Dep't of Health and Human Servs., to author (Feb. 12, 2008, 14:48:57 EST) (on file with author) ("No civil money penalties have been imposed on a covered entity for a violation of the Privacy Rule . . ."); see also Ctr. for Medicare & Medicaid Servs., U.S. Dep't of Health & Human Servs., CMS Enforcement Statistics Report: Open and Closed Cases by Type as of December 31, 2007, <http://www.cms.hhs.gov/Enforcement/Downloads/EnforcementStatistics-December2007.pdf> (last visited Apr. 8, 2008) (providing Security Rule statistics); Office for Civil Rights, U.S. Dep't of Health & Human Servs., Compliance and Enforcement: Numbers at a Glance, <http://www.hhs.gov/ocr/privacy/enforcement/numbersglance1207.html> (last visited Apr. 8, 2008) (providing Privacy Rule statistics).

145 See Office for Civil Rights, U.S. Dep't of Health & Human Servs., Compliance and Enforcement: Numbers at a Glance, <http://www.hhs.gov/ocr/privacy/enforcement/numbersglance1207.html> (last visited Apr. 8, 2008) (reporting 419 referrals to DOJ).

146 See Jonathan P. Tomes, *Individual Criminal Liability for HIPAA Violations: Who Is Potentially Liable? Or Should We Say, Who Isn't?*, J. HEALTH CARE COMPLIANCE, July-Aug. 2007, at 5, 5.

147 For instance, Janlori Goldman, head of the Health Privacy Project, is quoted as saying:

"The law was put in place to give people some confidence that when they talk to their doctor or file a claim with their insurance company, that information isn't going to be used against them They have done almost nothing to enforce the law or make sure people are taking it seriously. I think we're dangerously close to having a law that is essentially meaningless."

Rob Stein, *Medical Privacy Law Nets No Fines: Lax Enforcement Puts Patients' Files at Risk*, *Critics Say*, WASH. POST, June 5, 2006, at A1.

lamenting HHS's failure to engage in independent audits pursuant to its statutory authority.¹⁴⁸

Critics of HIPAA enforcement, supported by several security breaches, argue that HHS is not doing enough to ensure the protection of personal health information. A privacy advocacy group, called the Health Privacy Project, keeps a list of post-HIPAA newspaper stories that involve personal health information being compromised.¹⁴⁹ For instance, in October 2006, a laptop containing the personal health information of 38,000 members was stolen from the health care organization Kaiser Permanente.¹⁵⁰ In November 2006, a thief stole two computers from the Family Health Center in Jeffersonville, Indiana.¹⁵¹ These computers contained the names, addresses, billing and medical information, and social security numbers of over 7000 women who were being treated for breast or cervical cancer.¹⁵² In September 2006, a computer containing the medical information of several former military men and women was stolen from a hospital in New York City.¹⁵³ These are just a few of many stories involving invasion into the privacy of personal health information.

Concerns over the effectiveness of HHS enforcement led to a report released at a Senate hearing by the Government Accountability Office (GAO) in February 2007, which criticized the coordination of HHS in ensuring the privacy of medical information transmitted electronically.¹⁵⁴ The GAO noted that while HHS has initiated activities that were intended to address concerns related to PHI,¹⁵⁵ under the current system the goals of safeguarding personal health information will not be met.¹⁵⁶ The GAO recommended that HHS develop a plan

148 See *id.*

149 See HEALTH PRIVACY PROJECT, HEALTH PRIVACY STORIES (2007), http://www.healthprivacy.org/usr_doc/Privacystories.pdf.

150 See *Another Stolen Laptop Reported, Another Personal Info Scare*, DENVER CHANNEL.COM, Nov. 28, 2006, <http://www.thedenverchannel.com/news/10414015/detail.html>.

151 See Dick Kaukas, *Patient Data on Stolen Computers Unused*, COURIER-JOURNAL (Louisville, Ky.), Nov. 29, 2006, at 1A.

152 See *id.* It is unclear whether a Security Rule violation occurred here. The article reports that the computers had two layers of password protection, although it does not say whether the information was encrypted. See *id.*

153 See Graham Rayman, *Data on Veterans Missing*, NEWSDAY (New York, N.Y.), Nov. 3, 2006, at A17. The computers were stolen despite the fact that they were located in a locked room and in a locked hallway. See *id.*

154 See U.S. GEN. ACCOUNTABILITY OFFICE, GAO-07-238, HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY 10 (2007), available at <http://www.gao.gov/new.items/d07238.pdf>.

155 See *id.* at 27.

156 See *id.* at 28.

containing specific goals and deadlines for ensuring the protection of PHI.¹⁵⁷ Disagreeing with the GAO's recommendation, HHS claimed that the implementation of the Privacy Rule and Security Rule were adequate foundations as safeguards of PHI.¹⁵⁸

But even if the Privacy and Security Rules provide an adequate foundation to safeguard personal health information, questions remain about whether the current system of enforcement serves as an effective deterrent. Moreover, there is also the important policy question of whether the current enforcement process properly protects the interests of patients whose medical information is compromised due to a HIPAA Privacy or Security Rule violation.

Professors Hoffman and Podgurski argue that the current enforcement process fails both in terms of its deterrent effect and in its protection of aggrieved patients whose medical information is misappropriated.¹⁵⁹ Their solution is to amend the HIPAA enforcement procedure to include a private cause of action, which they contend would be the best way to effectively deter HIPAA violations while at the same time vindicating the rights of aggrieved patients.¹⁶⁰ Specifically, they propose that HIPAA be amended to include the following provision:

- (a) Any person aggrieved by any act of a covered entity in violation of this section may bring a civil action in a United States District Court.
- (b) The court may award—
 - (1) actual damages, but not less than liquidated damages in the amount of \$2500;
 - (2) punitive damages upon proof of willful or reckless disregard of the law;
 - (3) reasonable attorney's fees and other litigation costs reasonably incurred; and
 - (4) such other preliminary and equitable relief as the court determines to be appropriate.¹⁶¹

To justify this proposal, Hoffman and Podgurski point out that the underlying purpose of HIPAA privacy regulations is to protect patients. In their view, the current system undermines that purpose

157 See *id.* at 4 (stating that HHS should develop a plan that "identif[ies] milestones for integrating the outcomes of HHS's privacy-related initiatives" to "ensure that the key privacy principles in HIPAA are fully addressed.").

158 See *id.* at 47.

159 See Hoffman & Podgurski, *supra* note 11, at 354–56.

160 See *id.*

161 *Id.* at 383 (citing identical language in the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2724 (2000)).

because it disregards the potential hardships that a privacy breach can cause.¹⁶² Instead of exclusively relying on a government agency—which is susceptible to political influences and limited resources¹⁶³—to monitor enforcement, Hoffman and Podgurski assert that conferring a private cause of action would be more effective because the threat of lawsuits would put both financial and reputational pressures on covered entities to make sure that they comply with the Privacy and Security Rules.¹⁶⁴ Under the current system, covered entities may discover that since the penalties of a HIPAA violation are not severe, it may be cheaper not to comply.¹⁶⁵ Hoffman and Podgurski also emphasize that published judicial opinions could prevent future violations because they might clarify vague or confusing language in the Privacy and Security Rules.¹⁶⁶

Many (if not most) of the Privacy and Security Rule violations do not result in actual money damages.¹⁶⁷ Hoffman and Podgurski, however, point to several other privacy laws that provide a right to recover attorney's fees and costs even if the plaintiff suffered only minimal damages.¹⁶⁸ In fact, Hoffman and Podgurski's proposed amendment to HIPAA is identical to a provision in the Driver's Privacy Protection Act of 1994, which affords a private cause of action when a person knowingly and illicitly obtains, uses, or discloses personal information from a motor vehicle record.¹⁶⁹ They also cite the Privacy Act of 1974,¹⁷⁰ the Video Privacy Protection Act of 1988,¹⁷¹ the Electronic

162 *See id.* at 355.

163 Hoffman and Podgurski hypothesize that since government agencies have to make "resource-rationing" decisions, they have the tendency to allocate their resources to cases that they perceive to be especially important to the public welfare, and thus a complaint of a violation that affects only one person might be ignored. *See id.* at 355–56.

164 *See id.*

165 *See id.* at 383 ("[C]overed entities may have an incentive to conduct a cost-benefit analysis from which they conclude that because the cost of compliance is great and the risk of being penalized for a violation is very small, they should not aggressively invest in PHI security measures.").

166 *See id.* at 356.

167 For instance, in the George Clooney story discussed in the introduction of this Note, there was clearly a Privacy Rule violation even though Clooney did not suffer any monetary loss as a result of the violation. *See Lambert & Schweber, supra* note 1.

168 *See Hoffman & Podgurski, supra* note 11, at 354–55, 354 n.167.

169 *See supra* note 161 and accompanying text.

170 *See* 5 U.S.C. § 552a(g) (2000) (providing individuals with the right to recover attorney's fees, litigation costs, and a limit of \$1000 for a willful violation).

171 *See* 18 U.S.C. § 2710(c) (2000) (providing individuals with a right to recover actual damages, but not less than \$2500, punitive damages, preliminary and equitable relief, attorney's fees, and litigation costs).

Communications Privacy Act,¹⁷² and the Cable Communications Policy Act¹⁷³ in support of their argument that HIPAA should be brought in line with other privacy laws that allow private citizens to vindicate their rights in court.¹⁷⁴

Professors Hoffman and Podgurski make a compelling argument for a private cause of action—the threat of pricey and potentially embarrassing lawsuits would certainly deter noncompliance. Their argument also appeals to basic notions of fairness—intuitively, it seems only right for an entity that violates the law to compensate those who are harmed as a result. And certainly, given the numerous stories pertaining to privacy and security breaches, there is significant room for improvement of HIPAA compliance. Yet affording aggrieved persons a private cause of action only makes sense when the overall benefits outweigh the costs. It is not clear that a private cause of action would achieve that result.

B. *Why HIPAA Should Not Contain a Private Right of Action*

There are several practical, economic, and policy drawbacks to affording litigants a private cause of action for a Privacy or Security Rule violation. Recent enforcement figures suggest that the current enforcement process is continually improving its efficiency and effectiveness. The costs of HIPAA compliance may increase in the near future due to the possibility that other state courts might fall in line with *Acosta* and *Sorensen*. Conferring a federal private cause of action—especially one that includes liquidated damages—for a HIPAA violation would prove too costly to the health care system. The best course of action, at least for the time being, is simply to give

172 See *id.* § 2520 (2000 & Supp. V 2005) (providing individuals with a right to recover actual damages, punitive damages, equitable relief, attorney's fees, and litigation costs).

173 See 47 U.S.C. § 551(f)(2) (2000) (providing individuals with a right to recover actual damages or liquidated damages, punitive damages, attorney's fees, and litigation costs).

174 Currently, there is a bill in the Senate Committee on Health, Education, Labor and Pensions that, among other things, enhances the protection of health information by regulating the use, access, and disclosure of health information by all persons, not just covered entities. See Health Information Privacy and Security Act, S. 1814, 110th Cong. § 201(a)(1) (2007). The proposed bill provides a private cause of action for aggrieved individuals. See *id.* § 323 (providing for preliminary and equitable relief, the greater of compensatory damages or \$5000, punitive damages, and attorney's fees). The crux of the bill concerns the rights of individuals to access their health information, see *id.* §§ 101–105, and the implementation of safeguards to protect private health information. See *id.* §§ 111–114.

HHS and covered entities more time to improve the current system before making any drastic changes.

The most obvious problem with conferring a private cause of action for a HIPAA violation concerns the uncertainty as to whether judges and juries are best equipped to determine if a violation has even occurred. The *Acosta* and *Sorensen* cases are representative of the varying degrees of difficulty that courts will face if patients are allowed to sue after a HIPAA violation. If the liability for Faber in *Acosta* hinged merely on whether or not he violated HIPAA, then it would be a very easy case—obviously HIPAA’s Security Rule prevents a doctor from granting an employee access to EPHI for no apparent reason.

The *Sorensen* case is not as straightforward. The Privacy Rule does not mention *ex parte* communications with physicians, but it does provide that PHI may be disclosed pursuant to a discovery request or lawful process as long as reasonable efforts have been made by the requesting party to give the patient notice.¹⁷⁵ Courts have grappled with how to interpret HIPAA’s effect on the legality of *ex parte* communications. Some courts have held that *ex parte* communications with treating physicians are lawful as long as the Privacy Rule’s conditions for disclosure are met.¹⁷⁶ Other courts have reasoned that HIPAA disfavors *ex parte* communications,¹⁷⁷ and still others have held that since HIPAA does not specifically mention *ex parte* communications, only state law should determine the lawfulness of such activities.¹⁷⁸ The first interpretation is probably correct because the Privacy Rule regulates how PHI may be disclosed without patient authorization in a judicial proceeding, and it specifically articulates conditions that must be met before a disclosure of PHI is lawful without patient authorization.¹⁷⁹ Nevertheless, the discrepancies amongst various courts suggest that determining whether a HIPAA violation has occurred is not always a straightforward task.

The Privacy and Security Rules, by design, provide covered entities with discretion. For instance, the Privacy Rule mandates that cov-

175 See 45 C.F.R. § 164.512(e)(1)(ii) (2007).

176 See *Crenshaw v. MONY Life Ins. Co.*, 318 F. Supp. 2d 1015, 1029 (S.D. Cal. 2004); *Law v. Zuckerman*, 307 F. Supp. 2d 705, 707 (D. Md. 2004).

177 See *EEOC v. Boston Mkt. Corp.*, No. CV 03-4227, 2004 U.S. Dist. LEXIS 27338, at *20–21 (E.D.N.Y. Dec. 16, 2004) (“The strong policy underlying HIPAA would appear to trump the reasoning of those pre-HIPAA decisions that allowed defense counsel *ex parte* access to plaintiff’s treating physicians . . .”).

178 See *Smith v. Am. Home Prods. Corp. Wyeth-Ayerst Pharm.*, 855 A.2d 608, 623 (N.J. Super. Ct. Law Div. 2003) (“Because informal discovery is not expressly addressed under HIPAA, the courts should be governed by state law . . .”).

179 See 45 C.F.R. § 164.512(e).

ered entities have “appropriate” safeguards that are “reasonably” designed to protect health information from illicit uses.¹⁸⁰ The Security Rule requires covered entities to continually renew and modify their security precautions so as to afford EPHI “reasonable and appropriate protection.”¹⁸¹ HHS, the entity which drafted the Privacy and Security Rules, is better situated than judges and juries to decide whether particular safeguards are reasonable and appropriate. There is no doubt that Privacy and Security Rules are complex, and certainly their complexity should not be an excuse for covered entities to violate them. At the same time, however, there are clear benefits to allowing HHS and covered entities to work together on solutions to potential problems, rather than allowing courts to promulgate standards of care when they may not be qualified to do so.¹⁸²

Over and above the practical difficulties that a private cause of action would entail, the most significant drawback to a private cause of action is its potential economic impact on the health care industry. The possibility of litigation for privacy and security violations would surely compel covered entities to incorporate more legal fees and judgment awards into their budgets—costs that would in turn be passed on to the patients themselves. These costs would add to the already very high costs of HIPAA privacy compliance.

Complying with HIPAA’s Privacy and Security Rules requires not only considerable money, but also considerable time. HIPAA’s requirements are quite cumbersome—staffs have to be trained, privacy officers have to be employed, safeguards have to be implemented, policies have to be developed, and lawyers often have to be retained to help covered entities navigate the complex legal rules promulgated by HHS.¹⁸³ According to one study, the costs associated with implementing HIPAA ranged from a minimum of \$10,000 for a small physician group practice, to as much as \$14 million for a larger

180 *Id.* § 164.530.

181 *Id.* § 164.306(d)(3)(ii).

182 HHS and covered entities have a fairly high success rate at working out solutions. *See supra* Part II.A.

183 *See supra* Part I.A–B (discussing HIPAA Privacy and Security Rule requirements); *see also* Robert L. Barbieri, Editorial, *HIPAA: The Good, the Bad, and the Ugly*, 15 OBG MGMT., July 2003, at 8, 8, *available at* http://www.obgmanagement.com/pdf/1507/1507OBGM_Editorial.pdf (“In one respect, HIPAA might be aptly retitled ‘An Act to Ensure the Full Employment of Lawyers.’ The legislation is so complex that health-care providers, insurers, the government, and possibly even patients will need expert administrators and lawyers to help guide their actions.”); Virginia A. Smith & Dawn Fallik, *Doctors, Patients Grapple with Specifics of Privacy Rule*, PHILA. INQUIRER, Mar. 8, 2005, at A1 (“[HIPAA has] cost millions for training and paperwork, lawyers and compliance officers.”).

covered entity.¹⁸⁴ Moreover, the costs that hospitals have incurred for implementing HIPAA's privacy provisions are estimated to exceed \$22 billion.¹⁸⁵ The additional costs would be staggering if covered entities were faced with the threat of private litigation for each violation. Indeed, the threat of tort liability has already led to enormous costs for health care providers. Due to increased jury awards in malpractice claims and a shrinking malpractice insurance market, medical malpractice premiums have increased steadily since 1992.¹⁸⁶ Estimates suggest that in 2006, the medical tort system added over \$190 billion to the cost of health care.¹⁸⁷ That averages out to \$1700 to \$2000 per American household.¹⁸⁸ While the added costs associated with conferring a private cause of action are unknown, health care providers are already devoting significant resources to litigation, and such expenses have dramatically increased the cost of health care.

In addition to the increased economic costs inherent to litigation, important policy concerns must be taken into account in determining whether conferring a private cause of action is prudent. Covered entities already have spent many resources to ensure HIPAA compliance. By compelling covered entities to devote a substantial amount of additional resources to defend HIPAA privacy-related litigation, a private cause of action would necessarily entail a diversion of resources from another source. But do we really want doctors and hospitals fretting so much about patient privacy at the expense of caring for the sick and working towards medical breakthroughs? One doctor predicted that HIPAA's Privacy Rule would "complicate the work of all clinicians and strain the foundation of patient care: the physician-patient relationship."¹⁸⁹ Certainly, it must be undesirable to place a high value on medical privacy at the expense of the underlying purpose of the health care system.

Affording patients a private cause of action for a HIPAA violation may also adversely affect the progress of medical research. Covered entities are permitted to share health records with researchers if the patient gives permission, or if the covered entity de-identifies the health records.¹⁹⁰ Yet a private cause of action for a HIPAA violation

184 See Les Nunn & Brian L. McGuire, *The High Cost of HIPAA*, EVANSVILLE BUS. J., Aug. 4, 2005, at 29, 29.

185 See *id.*

186 See PAMELA VILLARREAL ET AL., NAT'L CTR. FOR POLICY ANALYSIS, MEDICAL MALPRACTICE REFORM 4-6 (2007), <http://www.ncpa.org/pub/bg/bg163/bg163.pdf>.

187 *Id.* at 8.

188 *Id.*

189 See Barbieri, *supra* note 183, at 8.

190 See *supra* notes 24-32 and accompanying text.

might deter covered entities from taking the risk that a patient's authorization was proper or that the medical record was adequately de-identified. But even if covered entities expend their financial and human resources to take such extra precautions, these resources would necessarily be diverted from other activities. Indeed, HIPAA compliance already has had significant impacts on the allocation of resources. According to Dr. Norman Fost of the University of Wisconsin School of Medicine, institutional review boards, which are responsible for overseeing research, "spend valuable time complying with HIPAA requirements that could be better spent on protecting the rights of research subjects."¹⁹¹ Shortly after the Privacy Rule first went into effect in April 2003, researchers were concerned that HIPAA's privacy requirements were so cumbersome that community hospitals and clinics would err on the side of caution and decide not to assist researchers.¹⁹² These concerns have proven true. A recent study has indicated that over two-thirds of epidemiologists have claimed that HIPAA has made their research activities more difficult.¹⁹³ One doctor even stated that HIPAA's privacy restrictions interrupted a twenty-five year study on stroke and heart disease.¹⁹⁴

The severe costs that society would incur if HIPAA were to confer a private cause of action should thus make Congress hesitate before bringing HIPAA in line with other privacy statutes. Consider, for instance, the Driver's Privacy Protection Act of 1994, which contains a remedy provision identical to the one that Professors Hoffman and Podgurski propose be added to HIPAA.¹⁹⁵ Under the Act, a plaintiff can sue an individual or a company that illicitly discloses private information from a motor vehicle record.¹⁹⁶ A private cause of action makes sense in this context because (1) the Act is fairly straightforward and thus easy to abide by, (2) knowingly and illicitly disclosing private information from a person's motor vehicle record is clearly bad behavior and usually self-serving, and (3) the costs of deterrence fall exclusively on the perpetrator. Consequently, plaintiffs who have suffered no actual damages as a result of a violation of the Act are able to collect liquidated damages and costs in court in order to deter per-

191 See Carla K. Johnson, *Patient Privacy Rules Said to Hinder Studies*, BOSTON GLOBE, Nov. 14, 2007, at A17.

192 See Sharon Machlis, *HIPAA Could Hamper Medical Research*, COMPUTERWORLD, May 5, 2003, at 19, 19.

193 See Johnson, *supra* note 191.

194 See *id.*

195 See *supra* note 161 and accompanying text.

196 See 18 U.S.C. § 2724(b) (2000).

petrators from bad conduct.¹⁹⁷ Unlike the Driver's Privacy Protection Act, however, HIPAA is undeniably complex, and not all HIPAA violations involve clearly bad behavior.¹⁹⁸ But the most significant difference is that under HIPAA, the deterrence costs, which would include both financial costs and a diminishment in the quality of the health care system, would be inevitably passed along to patients. Thus, the reasons why a private cause of action makes sense for a Driver's Privacy Protection Act violation do not support a private cause of action for a HIPAA violation.

Admittedly, many of the reasons proffered as to why HIPAA should not confer a private cause of action might aptly be described as criticisms of the Privacy and Security Rules themselves. Yet despite the unfortunate adverse effects on the physician-patient relationship and on medical research, HIPAA's Privacy and Security Rules may certainly be well worth their costs, especially since PHI is extremely valuable.¹⁹⁹ The larger question of whether HIPAA's privacy regulation is ultimately a good idea, however, is distinct from the question of whether a private cause of action makes sense.²⁰⁰ The answer to the

197 See *Kehoe v. Fidelity Fed. Bank & Trust*, 421 F.3d 1209, 1213 (11th Cir. 2005) ("Since liquidated damages are an appropriate substitute for the potentially uncertain and unmeasurable actual damages of a privacy violation, it follows that proof of actual damages is not necessary for an award of liquidated damages [after a violation of the Driver's Privacy Protection Act]. To us, the plain meaning of the statute is clear—a plaintiff need not prove actual damages to be awarded liquidated damages.").

198 Consider, for instance, the following case example on OCR's webpage:

At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.

Office for Civil Rights, U.S. Dep't of Health & Human Servs., Compliance and Enforcement: All Case Examples—Case #9, <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html#case9> (last visited Apr. 8, 2008). Here, the covered entity clearly violated the Privacy Rule's requirement that patients are entitled access to their health information at their request, see 45 C.F.R. § 164.502(a)(2) (2007), and HHS was able to work with the covered entity to ensure compliance. Granted, it would be unrealistic for HHS to work with every covered entity to implement effective plans, but it is not so clear, at least in the above scenario, that the threat of a lawsuit would have deterred the private practice from refusing to give the patient the requested information.

199 See *supra* notes 141–42 and accompanying text.

200 Professor Richard A. Epstein has argued that privacy regulation is unnecessary because "the provision of medical care can easily be organized by contract," and

former would require an extensive study on whether the benefits gained by regulation ultimately outweigh the costs imposed on the health care system, whereas the latter should only ask whether the added costs associated with a private cause of action exceed the benefits. While an individual remedy for a HIPAA violation would undoubtedly create added incentives both for covered entities to comply with HIPAA and for patients to be more proactive in recognizing HIPAA violations, the institutional costs of a private cause of action would be far-reaching and potentially have negative effects on basic tenets of the health care industry, including the physician-patient relationship and medical research. Because of such widespread effects, the question of whether HIPAA should have a private cause of action ought to be evaluated on an institutional level—the costs of a private cause of action to the entire health care industry must be less than the benefit that society would receive if HIPAA compliance were to increase.

Given the significant costs that a private cause of action would have on the health care industry, there would need to be compelling evidence that HIPAA compliance is so inadequate that a private cause of action would be superior to the current enforcement process. Recent news stories reporting privacy breaches²⁰¹ and the fact that there have been over 30,000 complaints submitted to HHS²⁰² indicate that there may be significant room for improvement in HIPAA compliance. At the same time, however, HHS has closed nearly eighty percent of the HIPAA-related complaints,²⁰³ and both the number of investigations and corrective actions achieved have increased on a yearly basis.²⁰⁴ The recent grant of subpoena power²⁰⁵ along with the independent audit of a hospital²⁰⁶ are further indications that HHS is taking HIPAA enforcement seriously and that such enforcement may

“[m]assive government regulation should not be introduced without profound evidence of system failure, which is not shown here.” Richard A. Epstein, *HIPAA on Privacy: Its Unintended and Intended Consequences*, 22 *CATO J.* 13, 28, 30 (2002). Epstein’s remarks were written before the Privacy and Security Rules came into effect. Yet the sizeable number of HIPAA-related complaints and the outcry over perceived inadequacies in HIPAA enforcement might undermine Epstein’s contention that it was not necessary for the federal government to regulate the privacy of health information. Nevertheless, whether the Privacy and Security Rules are the most efficient means to protect PHI remains a legitimate question.

201 See *supra* notes 149–53 and accompanying text.

202 See *supra* notes 92, 102 and accompanying text.

203 See *supra* notes 92, 103 and accompanying text.

204 See *supra* notes 95–96 and accompanying text.

205 See *supra* note 107 and accompanying text.

206 See *supra* note 108 and accompanying text.

be on the rise in the near future. Although a private cause of action would certainly increase the current level of compliance, a comparable level may be reached without having to burden the health care industry.

Even if enforcement of HIPAA is showing signs of growth, critics of the current system of enforcement might still contend that a private cause of action should be available right now because they believe that patients who suffer from a HIPAA violation are treated unjustly in that they are not compensated for their injuries.²⁰⁷ Yet allowing patients to sue would necessarily entail increased tort litigation expenses, which are already staggering for both health care providers and society at large.²⁰⁸ Despite any sense of justice achieved by allowing aggrieved individuals to recover money after a violation, the larger, more widespread injustice would be for society to suffer increased health care costs and setbacks to medical research and breakthroughs.

The preceding discussion is not meant to suggest that conferring a private cause of action for Privacy and Security Rule violations could never be a good idea. Rather, the point is to articulate several drawbacks of a private cause of action and to emphasize the benefits of the current system of enforcement. Indeed, a private cause of action might be warranted in the future if HHS were to become so overburdened with complaints that it lacked the resources to play a meaningful role in enforcement.²⁰⁹ In such a scenario, the case for a private cause of action would be bolstered if HIPAA's requirements became more lucid—either through amendments to the Rules and/or increased HHS guidance—because then courts would have an easier time in determining whether a violation has occurred. Currently, however, HHS is doing a reasonable job at HIPAA enforcement and the Privacy and Security Rules remain discretionary and complex. Even though recent news stories concerning privacy breaches have

207 See *supra* notes 159, 162 and accompanying text.

208 See *supra* notes 186–88 and accompanying text.

209 If we reach a point where HHS cannot respond to the public's complaints, then there will likely be enough political pressure to compel Congress to respond, especially given the existence of organizations that advocate increased health care privacy such as the Health Privacy Project. See *supra* note 149. As James Q. Wilson has argued, "The cost of effective political access has also been lowered by the existence within government, especially in Congress, of people who are sympathetic to consumerist . . . organizations [and] persons who either derive satisfaction for themselves or political rewards . . . from their ability to mount investigations or draft legislation in the regulatory area." JAMES Q. WILSON, *THE POLITICS OF REGULATION* 380 (1980).

caused quite a stir, the less newsworthy successes of the current system should not be overlooked.²¹⁰

The Privacy Rule has only been in effect since 2003, and the Security Rule since 2005. As covered entities have more time to adjust to the requirements and receive more guidance from HHS, their compliance will likely increase with time. Given the costs of HIPAA compliance and the possibility that these costs might increase if state courts start incorporating HIPAA as the standard of negligence,²¹¹ society would not benefit, and indeed would be harmed, by conferring a private cause of action.

CONCLUSION

Finding an adequate balance between the privacy of personal health information and the welfare of the health care system is an extraordinarily difficult task. The Privacy and Security Rules have caused drastic changes to the ways in which covered entities process, disclose, and protect health information. As Richard A. Epstein put it:

When we ask the larger question of how HIPAA works, it quickly becomes clear that it reverses what was once the ordinary presumption, which held that when you went to a doctor, you generally knew that the medical records could be used for any purpose which was reasonably related to your treatment or care, or to the overall assessment of the system.²¹²

The fundamental changes stemming from HIPAA have resulted in significant costs to the health care system, and have even had unintended consequences on medical research. A private cause of action for a Privacy or Security Rule violation would significantly increase these economic and opportunity costs, which would adversely affect patients. Consequently, society has an interest in keeping compliance costs down. At the same time, society has a strong interest in limiting the accessibility of personal health information, which is reflected in the general aims of the Privacy and Security Rules.

Recent security breaches have highlighted both the desirability and the vulnerability of health information, and instances of health

210 See Epstein, *supra* note 200, at 21 (“In some instances, computer glitches could result in the widespread if mistaken disclosure of confidential information. In other cases, hospital workers could leak information about the health conditions of celebrity patients. These cases dominate the public discourse, and the quieter successes of most activities is thereby overlooked.” (citation omitted)).

211 The same reasons proffered as to why HIPAA should not contain a private cause of action are also reasons why state courts should be hesitant to adopt a bright-line rule that a HIPAA violation constitutes negligence.

212 Epstein, *supra* note 200, at 20.

information being compromised suggest that there is still work to be done in protecting health information. Yet all signs indicate that HHS is ready for the task. When the costs associated with the threat of civil litigation in state courts are added, a federal private cause of action would overly burden covered entities, and indeed the entire health care system.

Conferring a private cause of action for a Privacy or Security Rules violation would undoubtedly be a drastic measure. The Privacy and Security Rules are still new, and given the potential costs to the health care system, Congress should give HIPAA enforcement and compliance more time to grow.

