DePaul Journal of Health Care Law

Volume 11
Issue 2 *Spring 2008*

Article 2

October 2015

The Privacy Rule: Are We Being Deceived?

Kendra Gray

THE PRIVACY RULE: ARE WE BEING DECEIVED?

Kendra Gray[*]

INTRODUCTION

The theft of a laptop from a Poughkeepsie, New York medical center in 2006 put the personal health information of nearly 260,000 patients at risk.[1] The breach occurred in June, but some patients were not notified until two months later.[2] Incidents like this raise the question: are our Privacy Rights truly being protected? The Federal Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") were enacted in April 2003 primarily to protect the privacy of our health information.[3] Since the implementation of the Privacy Rule, the U.S. Department of Health and Human Services ("HHS"), Office for Civil Rights ("OCR") has received thousands of complaints, but has not imposed a single civil fine and has prosecuted only two criminal cases.[4] Winston Wilkinson, Director of HHS, OCR has stated that "[HHS'] first approach to dealing with any complaint is to work for voluntary compliance, [and] so far it's worked out pretty well."[5] This Article argues that although the Privacy Rule has been a decent experiment, voluntary compliance alone is insufficient. Members of the health care industry are repeatedly pardoned for the mistakes they make with our personal information, while complainants are left without a remedy. Without real enforcement, there is little incentive for the heath care industry to comply with the law. If the Privacy Rule is to remain in place, something must be done to improve its effectiveness.

Part I of this Article provides an overview of the Health Insurance Portability and Accountability Act ("HIPAA"), including why the law was created and how it led to the development of the

---

[*] The Author worked as intern at the Department of Health and Human Services, Office for Civil Rights, Region V, from February 2006 to August 2006. The author has experience investigating and resolving Privacy Rule complaints.

[1] Health Privacy Project, *Health Privacy Stories*, at 4, http://www.healthprivacy.org/usr_doc/Privacystories.pdf (last visited March 1, 2007).

[2] *Id.*

[3] *See* The Privacy Rule, 45 C.F.R. §§ 160, 164, subparts A and E (2002).

[4] Rob Stein, *Medical Privacy Law Nets No Fines,* WASH. POST, June 5, 2006, at A1.

[5] *Id.*

Privacy Rule. Part II provides information about the purpose, application and enforcement of the Privacy Rule. Part III explains why HHS' emphasis on voluntary compliance is an inadequate method of ensuring the privacy of our health information. Part IV proposes methods for improving the enforcement of and compliance with the Privacy Rule.

I. BACKGROUND

Congress passed the Health Insurance Portability and Accountability Act ("HIPAA") in 1996 in response to "specific problems of availability and affordability of health insurance in the United States."[6] Although HIPAA lead to the creation of the Privacy Rule, Congress did not even consider the protection of privacy as a purpose of HIPAA.[7] Title I of HIPAA promotes the availability of health insurance by protecting health insurance coverage for workers and their families when they change or lose their jobs.[8] Title II of HIPAA promotes the affordability of health insurance by imposing anti-fraud provisions and by requiring the establishment of national standards for electronic heath care transactions.[9]

---

[6] H.R. REP. No. 104-496, at 70 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 1865, 1869. HIPAA was meant to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, [and] to simplify the administration of health insurance." H.R. REP. No. 104-496, at 1 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 1865, 1865.

[7] Marie C. Pollio, *The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579, 584 (2004); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 110 Stat. 1936 (1996) [hereinafter HIPAA]; H.R. REP. No. 104-496, at 66-67 (1996), *as reprinted in* 1996 U.S.C.C.A.N. at 1866.

[8] Health and Human Services, Centers for Medicare & Medicaid Services, *Health Insurance Reform for Consumers, Overview*, http://www.cms.hhs.gov/HealthIns ReformforConsume/Downloads/protect.pdf, at 1-2 (last visited March 1, 2007); Tracy Kania, *Toward HIPAA Compliance*, 85 EXTENDED CARE PRODUCT NEWS, 1, 13-15 (2003), *available at* http://www.extendedcarenews.com/article/1265.

[9] Health and Human Services, Centers for Medicare & Medicaid Services, *HIPAA-General Information, Overview*, http://www.cms.hhs.gov/HIPAAGenInfo/ (last visited March 1, 2007); Tracy Kania, *Toward HIPAA Compliance*, 85 EXTENDED CARE PRODUCT NEWS 1, 13-15 (2003), *available at* http://www.extendedcare news.com/article/1265 (last visited March 1, 2007).

A. Availability (Title I)

At the end of the twentieth century, almost forty million Americans lacked health insurance, while the cost of heath care was on the rise.[10] The majority of Americans who were insured were covered by employment-based health insurance.[11] Congress wanted to preserve that system,[12] but in order to encourage the public to maintain employment-based health insurance whenever it was offered, it was important to make sure that the public could depend on that form of coverage.[13]

Americans had specific concerns about employer-based health insurance.[14] For example, many Americans who received medical insurance from their employer were reluctant to take new jobs for fear of losing their health insurance coverage.[15] This "job-lock" occurred because employers or insurers imposed pre-existing condition exclusions on individuals when they changed jobs, which were often limited to specific periods of time, but could be permanent.[16] HIPAA solved this problem by requiring group health plans to credit previously carried insurance as "coverage towards any pre-existing condition limitation the plan would otherwise be permitted to impose"[17] and by prohibiting group health plans from excluding coverage from individuals based on their health status.[18]

---

[10] H.R. REP. No. 104-496, at 68, *as reprinted in* 1996 U.S.C.C.A.N. at 1868.

[11] H.R. REP. No. 104-496, at 74, *as reprinted in* 1996 U.S.C.C.A.N. at 1873-74. Sixty-two percent of Americans were covered by employment-based health insurance. Because of the cost factor, the rate of employment-based coverage ranged from ninety-two percent of workers in firms of 1,000-plus employees to only sixty-seven percent in the smallest firms of ten or fewer workers. H.R. REP. No. 104-496, at 68, *as reprinted in* 1996 U.S.C.C.A.N. at 1868.

[12] H.R. REP. No. 104-496, at 68, *as reprinted in* 1996 U.S.C.C.A.N. at 1869.

[13] H.R. REP. No. 104-496, at 68-69, 74, *as reprinted in* 1996 U.S.C.C.A.N. at 1868, 1874.

[14] H.R. REP. No. 104-496, at 68-69, *as reprinted in* 1996 U.S.C.C.A.N. at 1868.

[15] *Id.*

[16] Pollio, *supra* note 7, at 582; H.R. REP. No. 104-496, at 73-74, *as reprinted in* 1996 U.S.C.C.A.N. at 1873.

[17] *Id.;* H.R. REP. No. 104-496, at 74, *as reprinted in* 1996 U.S.C.C.A.N. at 1874.

[18] *Id.*; H.R. REP. No. 104-496, at 76, *as reprinted in* 1996 U.S.C.C.A.N. at 1876.

B. Affordability (Title II)

The rising cost of health care was made worse by two crucial sources: fraud and abuse and the burden created by medical paperwork.[19] HIPAA imposed anti-fraud provisions, which authorized the Secretary of HHS ("Secretary") and the Attorney General to "conduct investigations, audits, evaluations and inspections relating to the delivery of and payment for health care."[20] The act also imposed administrative simplification provisions, which would lead to the creation of a health information system by "establishing uniform standards for health information and requirements for the electronic transmission of certain health information."[21] The administrative simplification provisions ultimately required the Secretary to adopt national standards for electronic health care transmissions, code sets, identifiers and the security of health information.[22]

---

[19] Pollio, *supra* note 7, at 583; H.R. REP. No. 104-496, at 69, *as reprinted in* 1996 U.S.C.C.A.N. at 1869. The General Accounting Office (GAO) reported that as much as ten percent of total health care costs were lost to fraudulent or abusive practices by health care providers. *Id.*

[20] H.R. REP. No. 104-496, at 79-80, *as reprinted in* 1996 U.S.C.C.A.N. at 1879-80. In addition, The Secretary of HHS was required to establish a national health care fraud and abuse data collection program for reporting final adverse actions against health care providers, suppliers, or practitioners. The data bank would provide a source for up-to-date information that can be used in investigating fraud and abuse cases and used when providers or suppliers are seeking new licenses, renewal of licenses, or hospital privileges. H.R. REP. No. 104-496, at 92, *as reprinted in* 1996 U.S.C.C.A.N. at 1892-93.

[21] H.R. REP. No. 104-496, at 97, *as reprinted in* 1996 U.S.C.C.A.N. at 1897-98. The uniform standards would reduce health care spending by "enabling the public and private sectors to reduce paperwork, expose fraud and abuse, provide consumers with the information they need to compare health plans and services, and would be less burdensome for providers." H.R. REP. No. 104-496, at 97-98, *as reprinted in* 1996 U.S.C.C.A.N. at 1898-99. Any standard shall apply, in whole or in part to the following persons: (1) A health plan, (2) A health care clearinghouse, (3) A health care provider who transmits any health information in electronic from in connection with a transaction referred to in section 1173(a)(1). Pub. L. No. 101-191 (HIPAA) § 262. These persons are "covered entities."

[22] Health and Human Services, *Administrative Simplification Under HIPAA: National Standards for Transactions, Privacy and Security* (Oct. 2003), http://www.hhs.gov/news/press/2002pres/hipaa.html (last visited March 21, 2007); HIPAA § 262. The Secretary had no more than eighteen months after the date of the enactment of HIPAA to adopt such standards. HIPAA § 262. Entities then had no more than twenty-four months after the date on which the initial standard was adopted to comply. Small Health plans had thirty-six months to comply. *Id.* These standards

Merging this immense amount of health information into one format raised concerns over the confidentiality and privacy of the information. To allay these fears, HIPAA directed the Secretary to "adopt standards relating to the privacy of individually identifiable health information concerning the rights of individuals who are the subject of such information, the procedures for exercising such rights, and the authorized uses and disclosures of such information."[23]

II. THE PRIVACY RULE: PURPOSE, APPLICATION AND ENFORCEMENT

The directives contained in HIPAA led to the creation of the Privacy Rule.[24] HIPAA required the Secretary to recommend privacy measures to Congress within twelve months.[25] Congress also gave itself three years to develop legislation concerning the "privacy of individually identifiable health information," and mandated that if such deadline passed with no legislation, the Secretary would have to develop guidelines.[26] After Congress missed its deadline, Donna Shalala, HHS Secretary, issued the proposed Privacy Rule in November 1999 and the final Rule in December 2000.[27] Covered entities[28] were

---

were expected to provide a net savings to the health care industry of $29.9 billion over ten years. Health and Human Services, *supra*.

[23] H.R. REP. No. 104-496, at 100, *as reprinted in* 1996 U.S.C.C.A.N. at 1900; 65 Fed. Reg. 82,463 (Dec. 28, 2000); Pollio, *supra* note 7, at 583.

[24] 45 C.F.R. §§ 160, 164, Subparts A and E (2006).

[25] 42 U.S.C.A. § 1320d-2 (2007); Pub. L. No. 104-191 § 264 (1996). Not later than the date that is 12 months after the date of the enactment of this Act [Aug. 21, 1996], the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information. *Id.*

[26] Meredith Kapushion, *Hungry, Hungry HIPAA: When Privacy Regulations Go Too Far*, 31 FORDHAM URB. L.J. 1483, 1485 (2004); 42 U.S.C.A. § 1320d-2 (2007); Pub. L. No. 104-191 § 264 (1996). If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) [subsec. (a) of this section] not enacted by the date that is 36 months after the date of the enactment of this Act [Aug. 21,1996], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. *Id.*

[27] Kapushion, *supra* note 26, at 1485; 64 Fed. Reg. 59,918 (proposed Nov. 3, 1999); 65 Fed. Reg. 82,462 (Dec. 28, 2000); The 2000 Privacy Regulations were guided by five principles: 1) consumer control; 2) boundaries; 3) security; 4) accountability; and

required to comply by April 14, 2003[29] and small health plans (less than $5 million) were given until April 14, 2004 to comply.[30]

A. Purpose

As stated above, the Privacy Rule was born out of the need to protect the confidentiality of information after the implementation of the HIPAA administrative simplification provisions. Protecting privacy was an important issue for many Americans.[31] Before the Privacy Rule was enacted, a growing number of patients were concerned that their personal health information was not being protected.[32] Patients were nervous about where their medical information was going and who could access it.[33] Some patients were so concerned about the security of their health information that they began to "lie or withhold information from their [health care] providers, pay out-of-pocket for care, see multiple providers to avoid the creation of a consolidated record, or sometimes avoid care altogether."[34]

This concern stemmed from many factors including "the growth of the number of organizations involved in the provision of care and the

---

5) public responsibility. Marie Pollio, *The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579, 589 (2004). The Privacy Rule was modified slightly in 2002 after the Bush administration announced proposed modifications to the 2000 "final" privacy regulations, which, among other things, made pre-treatment consent optional and permitted incidental disclosures. 67 Fed. Reg. 53,182 (Aug. 14, 2002). "The proposed modifications collectively were designed to ensure that protections for patient privacy were implemented in a manner that maximized the effectiveness of such protections while not compromising either the availability or the quality of medical care." *Id.* Secretary Tommy Thompson issued the final rule in August 2002. *Id.*

[28] Covered entities are health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction covered by the Privacy Rule. 45 C.F.R. § 160.103 (2006).

[29] Kapushion, *supra* note 26, at 1485; 45 C.F.R. § 164.534 (2006).

[30] Kapushion at 1485; 45 C.F.R. § 160.103 (2006).

[31] A Wall Street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most about the coming century and "loss of personal privacy" was the first or second concern of twenty-nine percent of respondents. All other issues, such as terrorism, world war, and global warming had scores of twenty-three percent or less. 64 Fed. Reg. 59918, 59920 (Nov. 3, 1999).

[32] 65 Fed. Reg. 82,463 (Dec. 28, 2000).

[33] David Morantz, *HIPAA's Headaches: A Call for a First Amendment Exception to the Newly Enacted Health Care Privacy Rules,* 53 U. KAN. L. REV. 479, 481 (2005).

[34] Pollio, *supra* note 7, at 579.

processing of claims, the growing use of electronic information technology, increased efforts to market health care and other products to consumers, and the increasing ability to collect highly sensitive information about a person's current and future health status as a result of advances in scientific research."[35] Congress realized that high-quality health care requires the exchange of personal and often sensitive information between a patient and a health care provider and that it is essential that a patient is able to trust that the information he or she shared will be protected and kept confidential.[36]

The primary goal of the Privacy Rule is to provide consumers access to their health information and to prevent the inappropriate use of that information.[37] The Rule accomplishes this by "limiting the use and disclosure of certain individually identifiable health information, giving patients the right to access their medical records, restricting most disclosures of health information to the minimum necessary for the intended purpose, and establishing safeguards and restrictions regarding the use and disclosure of records for certain public responsibilities, such as public health, research and law enforcement."[38]

The Privacy Rule established, for the first time, a set of basic national privacy standards and fair information practices.[39] Almost every state had adopted one or more laws to safeguard privacy, but those laws varied from state to state.[40] Further, many state laws failed to provide basic protections such as ensuring a patient's legal right to see a copy of his or her medical record.[41] The Privacy Rule set a floor of rules for covered entities to follow[42] and only preempts less stringent

---

[35] 65 Fed. Reg. 82,463 (Dec. 28, 2000).

[36] *Id.*

[37] *Id.* The other goals are to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of health care, and to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals. *Id.*

[38] Privacy Rule; HHS, *supra* note 22.

[39] 65 Fed. Reg. 82,464 (Dec. 28, 2000). Before the Privacy Rule, privacy laws varied significantly from state to state and those laws generally applied to only part of the health care system. For example, many states adopted laws that protect the health information relating to certain health conditions such as mental illness, communicable diseases, cancer, HIV/AIDS and other stigmatized conditions. *Id.*

[40] 65 Fed. Reg. 82,463-82,464 (Dec. 28, 2000).

[41] *Id.*

[42] 65 Fed. Reg. 82,464 (Dec. 28, 2000).

state laws.[43] The Rule created a framework of protection that can be strengthened by both the federal government and by states as health information systems evolve.[44]

B. Application

Although the Privacy Rule may seem cumbersome, it governs only a small set of entities and transactions. Essentially, the Rule creates a blanket prohibition disallowing all covered entities from using or disclosing protected health information ("PHI").[45] PHI is defined as individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.[46]

There are exceptions to the blanket prohibition of the Privacy Rule.[47] For instance, a covered entity is permitted to use or disclose PHI to the individual or for treatment, payment, or health care operations.[48] A covered entity must also disclose PHI to OCR when OCR is investigating the covered entity's compliance with the Privacy Rule.[49] When the covered entity discloses PHI, it should disclose only that which is minimally necessary to accomplish the intended purpose of the disclosure or request.[50] The Rule provides several other

---

[43] 45 C.F.R. § 160.203 (2006). A regulation promulgated under paragraph (1) shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation. This means the Privacy Rule will not disturb more protective rules or practices. 65 Fed. Reg. 82,471 (Dec. 28, 2000).

[44] 65 Fed. Reg. 82,464 (Dec. 28, 2000).

[45] 45 C.F.R. § 164.502 (2006); Pollio, *supra* note 7, at 590. It is important to note that the Privacy Rule only regulates covered entities 45 C.F.R. § 160.102 (2006).

[46] 45 C.F.R. § 160.103 (2006); Pollio, *supra* note 7, at 590. PHI excludes education records covered by the Family Education Rights and Privacy Act; education records of adult students at postsecondary institutions, which are maintained by a health care professional and are used only in connection with the provision of treatment to the student; and employment records held by a covered entity in its role as employer. 45 C.F.R. § 160.102 (2006); Pollio, *supra* note 7, at 590.

[47] 45 C.F.R. § 164.502(a) (2006); Pollio, *supra* note 7, at 590.

[48] *Id.*

[49] *Id.*

[50] 45 C.F.R. § 164.502(b); Pollio, *supra* note 7, at 590. The "minimum necessary" requirement does not apply to disclosures to a health care provider for treatment, to individuals, or to OCR. *Id.*

exceptions and qualifications to the general prohibition against disclosing PHI.[51]

Besides controlling the use and disclosure of PHI, the Privacy Rule also allows individuals to obtain access to their PHI.[52] For example, a patient may request a copy of his or her medical records. An individual has a right to inspect and obtain a copy of her PHI and the covered entity must provide the access in a timely manner.[53] The covered entity may charge a reasonable, cost-based fee.[54] In addition, an individual may request that a covered entity restrict the use or disclosure of her PHI,[55] request an amendment to her PHI,[56] or request an accounting of all uses or disclosures of her PHI made by the covered entity.[57]

Lastly, the Privacy Rule mandates certain administrative requirements that a covered entity must follow such as "designating a privacy officer to oversee all privacy activities and receive complaints, training its workforce concerning proper privacy protections, creating reasonable safeguards to protected the privacy of PHI, creating a complaint process, documenting privacy policies and procedures, imposing sanctions against employees who violate privacy policies,

---

[51] A covered entity must obtain an authorization if it is seeking to engage in marketing activities or to use or disclose psychotherapy notes. 45 C.F.R. § 164.508; A covered entity may use or disclose PHI in the making and use of facility directories, in involving others in the individual's care, or for notification purposes provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure. 45 C.F.R. § 164.510; A covered entity may use or disclose PHI without the written authorization of the individual if it is required by law, for public health activities, for disclosures about victims of abuse, neglect or domestic violence, for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, for certain information about decedents, for information for donation and research purposes, to avert a serious threat to health or safety, for specialized government functions, or for workers' compensation. 45 C.F.R. § 164.512; Pollio, *supra* note 7, at 590-591. Other requirements exist relating to the use and disclosure of PHI. Prior to disclosing PHI, a covered entity must "verify the identity of the person requesting the PHI and its authority to do so, identify those employees who need access to PHI to carry out their duties and limit access to only those so identified, and implement policies and procedures to limit disclosures to the minimum necessary to accomplish the purpose of the disclosure." 45 C.F.R. § 164.514; Pollio, *supra* note 7, at 591.

[52] 45 C.F.R. § 164.524; Pollio at 591.

[53] 45 C.F.R. § 164.524(a), (c)(3); Pollio at 591.

[54] 45 C.F.R. § 164.524(c)(4).

[55] 45 C.F.R. § 164.522; Pollio at 591.

[56] 45 C.F.R. § 164.526; Pollio at 591.

[57] 45 C.F.R. § 164.528; Pollio at 591.

refraining from intimidating or hostile acts against complainants, and mitigating any harmful effect due to the use or disclosure of PHI."[58]

C. Enforcement

There is no private right of action for alleged violations of the Privacy Rule, which means individuals cannot file lawsuits for HIPAA violations.[59] In the proposed privacy rules, HHS expressed its concern that HIPAA lacked a private right of action,[60] but Congress disregarded those suggestions. In a recent decision, *Acara v. Banks*, the U.S. Court of Appeals, Fifth Circuit, affirmed that Congress did not intend for private enforcement of HIPAA and that every district court that had considered the issue agreed that the statute did not support a private right of action.[61] Instead, OCR is responsible for the administration and enforcement of the Privacy Rule.[62]

---

[58] 45 C.F.R. § 164.530; Pollio at 592.

[59] Jamie Lund, *ERISA Enforcement of the HIPAA Privacy Rules*, 72 U. CHI. L. REV. 1413, 1413 (2005). Author explains that HIPAA does not contain an explicit private right of action and that courts have refused to infer a private right of action. Footnote six gives examples of courts finding no private right of action. *Id.*

[60] Standards for the Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,923 (Nov. 3, 1999). HHS was troubled that the rule's penalty structure did not reflect the importance of privacy protections and the need to maintain individuals' trust in the system. HHS called for federal legislation to ensure the privacy protection for health information will be strong and comprehensive. *Id.* at 59,924.

[61] *Acara v. Banks*, 470 F.3d 569, 571 (5th Cir. 2006). The court stated, "Private rights of action to enforce federal law must be created by Congress. HIPAA has no express provision creating a private cause of action, and therefore we must determine if such is implied within the statute. . . . HIPAA limits enforcement of the statute to the Secretary of Health and Human Services. Because HIPAA specifically delegates enforcement, there is a strong indication that Congress intended to preclude private enforcement." *Id.*

[62] Statement of Delegation of Authority, 65 Fed. Reg. 82,381 (Dec. 28, 2000); 65 Fed. Reg. 82,472 (Dec. 28, 2000); HHS, *Fact Sheet: Protecting the Privacy of Patients' Health Information* (April 14, 2003), *available at* http://www.hhs.gov/news/facts/privacy.html.

The enforcement process is complaint-driven, [63] meaning that any individual who believes that a covered entity is not complying with the Privacy Rule may file a complaint with OCR. [64] OCR may investigate complaints, which could include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged violation.[65] It is important to note that OCR is not required to investigate every complaint.[66] Also, OCR has the authority to initiate investigations on its own, but that rarely occurs.[67]

The Privacy Rule outlines a number of penalties for noncompliance and wrongful disclosure of PHI. The Rule permits civil money penalties ("CMPs") for failure to comply with its requirements and standards, ranging from fines of $100 to $25,000 per person per violation.[68] HIPAA also authorizes the imposition of criminal penalties

---

[63] Pollio, *supra* note 7, at 592; 45 C.F.R. §160.306. Privacy Rule complaints are most often filed against the following types of covered entities (from highest number of complaint): private health care practices (i.e., physician offices), general hospital, outpatient facilities, group health plans and health insurance issuers, and pharmacies. Winston Wilkinson, The Office for Civil Rights & Health Care Privacy, *Remarks for the Twelfth National HIPAA Summit, Hyatt Regency on Capital Hill*, April 10, 2006, p. 4 *available at* http://www.hhs.gov/ocr/HIPAASummitPresentation041006.doc. Typically, Privacy Rule complaints generally involve allegations of the impermissible use or disclosure of an individual's identifiable health information, the lack of adequate safeguards to protect identifiable health information, refusal or failure to provide the individual with access to or a copy of his or her records, disclosure of more data than is minimally necessary to satisfy a request for information, or failure to have the individual's valid authorization for a disclosure that requires one. *Id.*

[64] 45 C.F.R. §160.306(a). Covered entities are also supposed to have a compliance officer to whom complaints may be reported; Angela Stewart, *HIPAA-An Attempt to Protect Individually Identifiable Health Information*, 28 WYO. L. 26, 29 (2005); 45 C.F.R. § 164.530(a)(1)(ii); Pollio, *supra* note 7, at 592. OCR includes instructions on its website about how to file a complaint. *See generally*, HHS, OCR, *Fact Sheet: How to File a Health Information Privacy Complaint with the Office for Civil Rights*, *at* http://hhs.gov/ocr/privacyhowtofile.htm (last visited March 16, 2007); There are certain requirements for filing a complaint, such as the complaint must be in writing; the complaint must name the person that is the subject of the complaint and describe the act or omission complained of occurred; and the complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission occurred. 45 C.F.R. §160.306(b).

[65] 45 C.F.R. §160.306(c).

[66] *Id.*

[67] 45 C.F.R. §160.308(c); "HHS has conducted just a 'handful' of compliance reviews." Stein, *supra* note 4.

[68] 45 C.F.R. §160.404 (b)(1)(i-ii); A penalty may not be imposed if it is established that the person liable for the penalty did not know, and by exercising reasonable

for "any person that knowingly misuses a unique health identifier, or obtains or discloses individual identifiable health information," which include fines up to $250,000 and ten years imprisonment.[69] HHS enforces the CMPs, while the U.S. Department of Justice enforces the criminal penalties.[70]

On February 16, 2006, HHS published the Final HIPAA Administrative Simplification Enforcement Rule ("Enforcement Rule"), which took effect on March 16, 2006.[71] The Enforcement Rule amended the "existing rules relating to the investigation of noncompliance to make [the rules] apply to all of the HIPAA Administrative Simplification rules, rather than exclusively to the privacy standards."[72] The Enforcement Rule did not alter substantially the Privacy Rule, rather it served to "clarify and elaborate" requirements for determining and counting violations, calculating and establishing liability for CMPs, and procedural issues, such as conduct of the hearing and the appeal process.[73] The Enforcement Rule did, however, alter how CMPs are issued.[74] If a complaint is not resolved informally, and OCR determines a CMP is warranted, OCR will send the covered entity a Notice of Proposed Determination.[75] The Notice includes information such as the violations found and the amount of the proposed CMP, and it allows the covered entity time to respond.[76] The Enforcement Rule also provides that CMPs may only be imposed on a covered entity - not an employee of the covered entity or the covered

---

diligence would not have known, that such person violated the provision. 42 U.S.C. § 1320d-5(b)(2).

[69] Standards for Electronic Transactions, 65 Fed. Reg. 50,312, 50,313 (Aug. 17, 2000); 42 U.S.C. § 1320d-6(b).

[70] HIPAA Administrative Simplification: Enforcement; Final Rule, 71 Fed. Reg. 8390 (Feb. 16, 2006). Although the statute includes both penalties, a person can only receive either the civil or the criminal penalty. 42 U.S.C. § 1320d-5(b)(1); Sonia W. Nath, *Relief for The E-Patient? Legislative and Judicial Remedies to Fill HIPAA's Privacy Gaps*, 74 GEO. WASH. L. REV. 529, 545-546 (2006).

[71] *See generally,* HIPAA Administrative Simplification: Enforcement; Final Rule, 71 Fed. Reg. 8390 (Feb. 16, 2006).

[72] *Id.*; The Enforcement Rule applies to the HIPAA Electronic Data Interchange (EDI) rules, the HIPAA privacy rules, the HIPAA security rules, and the HIPAA unique identifiers. Segal, *Capital Checkup, Final HIPAA Enforcement Rule* (March 15, 2006), *available at* http://www.segalco.com/publications/capitalcheckup/031506no2.html#two.

[73] Segal, *supra* note 72; Wilkinson, *supra* note 63, at 4.

[74] Wilkinson, *supra* note 63, at 5.

[75] 45 C.F.R. § 160.420; Wilkinson, *supra* note 63, at 5.

[76] Wilkinson, *supra* note 63, at 5.

entity's agent - and if a CMP becomes final, the Secretary will notify the public.[77]

Although the Privacy Rule contains penalties and the Enforcement Rule was recently enacted, the Privacy Rule still *requires* voluntary compliance first, no matter how egregious the conduct was (except for criminal conduct).[78] The Rule states, "if an investigation of a complaint or a compliance review indicates noncompliance, the Secretary **will** attempt to reach a resolution of the matter satisfactory to the Secretary by informal means.[79] Informal means may include demonstrated compliance or a completed corrective action plan or other agreement."[80] The Rule provides that, "enforcement activities will include working with covered entitles to secure voluntary compliance through the provision of technical assistance and other means; responding to questions regarding the regulation and providing interpretations and guidance; responding to state requests for exception determinations; investigation compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution."[81]

II. VOLUNTARY COMPLIANCE IS INADEQUATE

There is a sharp divide between those who support and those who oppose HHS' emphasis on voluntary compliance. The government has stood by its decision to promote voluntary compliance and has a strong ally in the health care industry. Conversely, patients and privacy advocates feel that the emphasis on voluntary compliance

---

[77] 45 C.F.R. § 160.426; Wilkinson, *supra* note 63, at 6.

[78] The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable administrative simplification provisions. The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable administrative simplification provisions. 45 C.F.R. §160.304; "Our approach will be to seek informal resolution of complaints whenever possible, which includes allowing covered entities a reasonable amount of time to work with the Secretary to come into compliance before initiation action to seek civil monetary penalties." 65 Fed Reg. 82,601; 45 C.F.R. §160.312 (2006), 65 Fed. Reg. 82,601; As to enforcement, a covered entity will not necessarily suffer a penalty solely because an act or omission violates the rule. As we discuss elsewhere, the Department will exercise discretion to consider not only the harm done, but the willingness of the covered entity to achieve voluntary compliance," "the Secretary will encourage voluntary efforts to cure violations of the rule." 65 Fed. Reg. 82603.

[79] 45 C.F.R. §160.312.

[80] *Id.*

[81] 65 Fed. Reg. 82,472 (Dec. 28, 2000).

has taken all of the meaning out of the law. Although there is much debate, statistics and personal accounts reveal that voluntary compliance is the wrong approach to protecting the privacy of our health information.

A. HHS and the Heath Care Industry Support Voluntary Compliance

On April 10, 2006, Winston Wilkinson, Director of HHS, OCR, stated that OCR "will continue to seek voluntary compliance as our primary way to resolve cases, as the most efficient use of our resources and the most effective means of obtaining meaningful and prompt compliance from covered entities."[82] HHS is not alone in its views. In general, those who work in the health care industry agree that voluntary compliance is the best way to enforce the Privacy Rule. A *Washington Post* staff writer reported that, "Representatives of hospitals, insurance companies, health plans and doctors [have] praised the administration's emphasis on voluntary compliance, saying it is the right tack, especially because the rules are complicated and relatively new."[83] "It has been an opportunity for hospitals to understand better what their requirements are and what they need to do to come into compliance," said Lawrence Hughes of the American Hospital Association.[84] In addition, Larry S. Fields, president of the American Academy of Family Physicians declared, "I applaud HHS for taking this route. We're more used to the government coming down with a heavy hand where it's unnecessary."[85]

B. Privacy Advocates and Patients Oppose Voluntary Compliance

Privacy advocates feel differently about HHS' policy of voluntary compliance. Some privacy advocates think that the "lack of civil fines has sent a clear message that health practitioners and organizations have nothing to fear if they violate HIPAA."[86] "[The Privacy Rule] is not being enforced very vigorously. No one is afraid of being fined or getting bad publicity. . . . As long as [covered entities]

---

[82] Wilkinson, *supra* note 63, at 6.
[83] Stein, *supra* note 4.
[84] *Id.*
[85] *Id.*
[86] *Id.*

respond [to OCR], they essentially get amnesty," declared William R. Braithwaite of the eHealth Initiative and Foundation, a nonprofit research and advocacy organization.[87] Another privacy advocate affirmed, "Basically, with the way things are right now, you have the right to whine to a federal agency. It's not exactly the most useful way to enforce problems."[88] The president of a health privacy consulting firm opined, "Enforcement is a farce. . . . There is no funding for what we call the HIPAA police. It's a joke because there aren't any HIPAA police."[89] Further, Janlori Goldman, a health care privacy expert at Columbia University stated, "[HHS has] 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."[90]

C. HHS' Policy of Voluntary Compliance is Ineffective and Insignificant

There is extensive evidence supporting the claim that HHS' policy of voluntary compliance is unsuccessful and meaningless. Surveys of the health care industry prove the lack of compliance with the Privacy Rule. In addition, complaint statistics demonstrate that OCR is not adequately enforcing of Rule. OCR has investigated only a fraction of the complaints it has received, and of those, it has resolved the complaint in favor of the health care provider or institution every time. It is clear that the government favors covered entities. The lack of compliance and lack of enforcement hurts those whom the Rule was intended to protect. Many Americans have been victims of Privacy Rule violations and their stories demonstrate the harmful and serious consequences that result from non-compliance with the Rule.

1. Statistics Prove Lack of Success

---

[87] *Id.*

[88] Heather Hayes, *HIPAA: Best if used by. . .*, Government Health IT (June 12, 2006), *available at* http://www.govhealthit.com/article94795-06-12-06-Print. Statement made by Dr. Deborah Peel, Texas psychiatrist and chairwoman of the Patient Privacy Rights Foundation.

[89] Bob Sullivan, Blog, The Red Tape Chronicles, *Health Care Privacy Law: All Bark, No Bite?* (October 24, 2006), *available at* http://redtape.msnbc.com/2006/10/two_years_ago_w.html.

[90] Stein, *supra* note 4.

Data supports those who disagree with HHS' focus on voluntary compliance. A recent survey by the American Health Information Management Association found that hospitals and other providers are still not fully complying with the Privacy Rule and that the level of compliance is falling.[91] That is inexcusable because, if anything, compliance should be increasing. Covered entities received enough time to learn the requirements of the Privacy Rule and to implement policies to ensure compliance.[92] These health care providers and organizations have been aware of the Privacy Rule since it was enacted in December 2000. Further, the majority of covered entities were required to comply with the Rule by April 2003.

Other studies have confirmed a lack of compliance with the Rule. For example, in the summer of 2006, Phoenix Health Systems and the Healthcare Information and Management Systems Society's semi-annual survey on HIPAA compliance in the U.S. health care industry found that a substantial percentage of providers (twenty-two percent) and payers (thirteen percent) remain noncompliant with the Privacy Rule regulations.[93] At least one-third of the noncompliant organizations reported that they would need seven months or longer to implement the Privacy Rule regulations.[94] Another one-third of the organizations did not even know when they would be compliant.[95] Arguably, such a large percentage of covered entities have not come into compliance because they know they will not face any serious repercussions for violating the Rule.

HHS has attempted to sidestep the subject of compliance by boasting about how many cases it has resolved. At the Twelfth National HIPAA Summit, Mr. Wilkinson stated that from April 2003 to March 2006, OCR had received 18,900 complaints and of those,

---

[91] Stein, *supra* note 4.

[92] "What a health plan or covered health care provider must do to comply with the rule is clear, and the two-year delayed implementation provides a substantial period for trade and professional associations, working with their members, to come into compliance with them." 65 Fed. Reg. 82,472 (Dec. 28, 2000).

[93] HIPAAdvisory, *US Healthcare Industry HIPAA Compliance Survey Results: Summer 2006*, *available at* http://www.hipaadvisory.com/action/surveynew/results/summer2006.htm (last visited March 16, 2007). 220 health care industry representatives (Providers and Payers) completed the survey. The data showed that even among "compliant" organizations, significant implementation gaps remained in certain areas, including establishing Business Associate Agreements, monitoring internal Privacy compliance, and maintaining "minimum necessary" information disclosure restrictions.

[94] *Id.*

[95] *Id.*

seventy-two percent had been resolved.[96] Resolving nearly three-fourths of all complaints sounds like a success, but that still leaves 5,292 individuals who believe their privacy rights were violated and who remain unsure about how or whether OCR will resolve their complaints. In addition, Mr. Wilkinson failed to mention that almost half of those complaints were not even eligible for investigation.[97] Including these ineligible complaints inflates OCR's supposed success with resolving complaints. Furthermore, of those complaints that were actually investigated, OCR found in favor of the covered entity every time.[98]

These statistics prove that OCR is not taking complainants' concerns seriously.[99] Dr. Deborah Peel, chairwoman of the Patient Privacy Rights Foundation, stated, "Our experience has been that complaints are being dismissed without any real investigation and very few of them are sent to the Department of Justice for enforcement."[100] The editor and publisher of the *Health Information Privacy/Security Alert*, Dennis Melamed, observed that "these statistics raise a lot more questions than they answer. For example, does this mean that concerns

---

[96] Wilkinson, *supra* note 63, at 4.

[97] Emails from Patrick Hadley, Senior Advisor of HIPAA Privacy Outreach, HHS, OCR (on file with author). A complaint would not qualify for investigation of a covered entity due to problems such as a lack of jurisdiction over the entity named in the complaint, untimely filing of the complaint, or allegations in the complaint that do not constitute violations of the Privacy Rule. *Id.* More recent data indicates that as of September 30, 2006, OCR had received a total of 22,664 Privacy Rule complaints, and had resolved seventy-six percent of these cases. Approximately 11,700 complaints were closed after a review determined that they did not present a case that qualified for investigation of a covered entity. This means that OCR did not investigate over half of the complaints it received. By September 30, 2006, OCR had investigated and closed approximately 5,400 complaints that were actually eligible for investigation. OCR calls these core complaints. Of these core complaints, OCR took enforcement action by informal means in approximately 3,700 cases (sixty-eight percent of the core complaints received). In the remaining 1,700 cases (thirty-two percent of the core complaints received), OCR found that the covered entity had not failed to comply with the Privacy Rule. Essentially, OCR found in favor of the covered entity in every case that it investigated and there are still 5,564 complainants waiting to find out how their complaint will be resolved. *Id.*

[98] *Id.*

[99] Heather Hayes, *Most Privacy Complaints are not Investigated*, Government Health IT, Dec. 18, 2006, *available at* http://www.patientprivacyrights.org/site/News2?id=6689&page=NewsArticle.

[100] *Id.*

over medical privacy are overblown? Or does it mean that the HIPAA privacy rule does not cover everyone it should?"[101]

HHS is very serious about resolving complaints by informal means, but from these statistics, it may be difficult to prove whether the privacy of our health information is more or less protected since the inception of the Privacy Rule. On October 24, 2006, a blogger from Omaha, Nebraska wrote, "no one can estimate the true number of violations" because from her work experience, "there is little enforcement of [the Rule] and it is not uncommon for employees to do with information as they please as little is monitored."[102]

What is certain is that since April 2003, thousands of Americans have complained to OCR that their privacy rights were violated.[103] These complaints range from nearly harmless to particularly egregious. Complainants have described everything from "unlocked cabinets containing personal information to nurses who announce patient data too loudly in waiting rooms."[104]

2. Examples of Recent Privacy Rule Violations

While thousands of people have had their privacy rights violated since the inception of the Privacy Rule, it is likely that many have no idea that their PHI was put in jeopardy because it is likely that more Privacy Rule violations occur than are actually reported. The Health Privacy Project compiles news stories about incidents affecting the privacy of health information, many of which occurred after April 2003.[105] For instance, on November 15, 2006, a news station reported that investigators discovered the PHI of over 200 people in unlocked garbage dumpsters outside Walgreens, CVS and other pharmacies in the Houston area.[106] The investigators found "prescription labels, pill bottles and computer printouts listing PHI."[107] In another instance, a primary care clinic in Sorora, California "released the Social Security

---

[101] Dennis Melamed, *Less Than 25% of Medical Privacy Complaints Merit Further HHS Investigation*, Health Information Privacy/Security Alert HIPAA Enforcement Statistics (December 2006), *available at* http://www.melamedia.com/0001%20HIPAA%20Stats.htm.

[102] Sullivan, *supra* note 89.

[103] Hadley, *supra* note 97.

[104] Sullivan, *supra* note 89.

[105] Health Privacy Project, *Health Privacy Stories, available at* http://www.healthprivacy.org/usr_doc/Privacystories.pdf (last visited March 15, 2007).

[106] *Id.* at 2.

[107] *Id.*

numbers of twenty-two veterans to at least two patients signing in for appointments."[108] In August 2006, *Wired Magazine* featured a story about an "Indiana-based consultant [who] was able to download the names, Social Security numbers and dates of birth for between 5,600 and 23,000 Georgetown University Hospital patients when he accidentally discovered the unsecured data on the website of e-prescribing vendor InstantDx."[109]

Some victims discovered the Privacy Rule violation almost immediately after the breach. For example, on October 29, 2004, the *New York Daily News* reported that an "emergency medical technician was suspended after sharing a patient's medical record with friends as a joke. The medical technician found the patient's medical circumstance funny, and stole the medical record from the ambulance, scanned it, and e-mailed it to friends and colleagues."[110] A blogger from Mission Viejo, CA wrote on October 24, 2006, "[HIPAA] is a great big joke! I was given two bottles of medication [that] were not mine and did not realize it until I got home. I phoned the pharmacy and they said to bring them back. No apology, nothing. I sent a complaint to [OCR] and they mailed me a letter six months later saying that the pharmacy did not make that mistake. I don't have time to battle that lie! They gave me heart medication and I don't have a heart problem!"[111]

These stories illustrate that a large portion of the health care industry is not complying with the Privacy Rule. Many of these covered entities are large corporations, such as pharmacies and hospitals, which have all the resources necessary to come into compliance with the law. There is no excuse for noncompliance.

3. **HHS Favors Covered Entities**

Complaint statistics and privacy stories also demonstrate that OCR is slow in resolving core complaints and that OCR favors covered entities over complainants. HHS does not disclose details about specific complaints, but the examples above should sufficiently demonstrate that since the implementation of the Privacy Rule, many covered entities have violated the Privacy Rule.[112] It is clear that there have been incidents in which covered entities have deserved more than

---

[108] *Id.* at 3.
[109] *Id.* at 4.
[110] *Id.* at 9.
[111] Sullivan, *supra* note 89.
[112] *Id.*

a slap on the wrist. In some of the more serious situations, covered entities should have been fined. It is absurd that for every privacy complaint OCR deemed "eligible for investigation," OCR either found that the covered entity did not violate the Privacy Rule or that the situation had been resolved through informal means.

The manner in which OCR "resolves" complaints through informal means should not even be considered corrective action or mitigation. OCR is often satisfied that a covered entity has come into compliance if the covered entity issued the complainant a letter of apology. Another example of an acceptable informal resolution is when the covered entity sanctions its employee who violated the Privacy Rule by placing a disciplinary note in his or her file. OCR does not have the authority to tell a covered entity to fire an employee. Retraining the covered entity's staff has also been interpreted as corrective action, which is curious because the Privacy Rule requires training in the first place.[113] For the most part, the covered entity decides how to penalize its employees who broke the law and OCR accepts the chosen method as corrective action.

Complainants do not receive a remedy through voluntary compliance. The complainant is never made whole, which is illustrated by the following incident. A patient complained to OCR alleging that a hospital employee, who was also a relative, had looked up her medical records without permission and then shared the information she discovered with another family member.[114] OCR began its investigation by asking for copies of the hospital policies and procedures on access to medical records by employees.[115] The hospital did not fire the employee who impermissibly accessed the complainant's medical records.[116] Instead, the hospital gave the employee a written warning and additional HIPAA training.[117] The hospital privacy officer sent OCR a package of materials including a letter explaining the results of its internal investigation and copies of the hospital's privacy policies.[118] The privacy officer explained the corrective action it took and described the disciplinary action taken

---

[113] 45 C.F.R. § 164.530(b)(1) (2006).

[114] *What One Hospital Privacy Officer Learned During a Surprise OCR Investigation*, HIPAA Compliance Strategies, AIS Compliance (Sep. 2005), *available at* http://www.aishealth.com/Compliance/Hipaa/RPP_Hospital_Privacy_Officer_Surprise.html.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

against its employee.[119] OCR was satisfied with the hospital's response and closed the case.[120]

Here, the complainant's privacy rights were violated and she got nothing as compensation. The only satisfaction she received was knowledge that the employee was warned and underwent more HIPAA training. With voluntary compliance, the wrong and the penalty are not equal. In this example, if the hospital had been fined, it is more likely that the complainant would have felt that the hospital was truly being penalized. Moreover, the hospital would have understood that OCR takes Privacy Rule complaints seriously.

IV. PROPOSALS: HOW TO ENSURE TRUE ENFORCEMENT OF THE PRIVACY RULE

A. Proposal #1: Amend or Revise the Current Law

1. Problem: The Structure of the Privacy Rule is Flawed

The current structure and implementation of the Privacy Rule favors covered entities, which is unfortunate because the Rule was created to protect the privacy of consumers. Covered entities do not need protection; they are in the position of power. Under the current structure of the Rule, even when there is a clear violation, violators are told to right their wrongs. The voluntary compliance approach leaves nothing to compel the health care industry to comply. Secretary Shalala was right when she said that covered entities will take their responsibilities seriously only if HHS puts the force of law behinds its rhetoric.[121]

OCR's focus on voluntary compliance is not by choice; rather it is what the Privacy Rule requires. When OCR receives a complaint from an individual alleging a violation of the Privacy Rule, OCR **must**

---

[119] *Id.*

[120] *Id.*

[121] On September 11, 1997, Secretary Shalala presented to Congress her recommendations for protecting health information including, "Requirements to protect individually identifiable health information must be supported by real and significant penalties for violations. We recommend federal legislation that would include punishment for those who misuse personal health information and redress for people who are harmed by its misuse. Only if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibilities seriously." 64 Fed. Reg. 59,923 (Nov. 3, 1999).

first seek voluntary compliance.[122] Not only is this policy ineffective, but it is difficult to imagine any other law that gives such leeway to the violator. With other laws, provable violations usually lead to penalties. Generally speaking, if a person commits a crime, he is punished by imprisonment, community service, or fines. A person cannot rob a bank and then give the money back to avoid going to jail. He does not have the option of apologizing to his victim or undergoing a refresher course about the law.

Under the Privacy Rule, people are left with only one option when they believe their privacy rights have been violated, which is filing a complaint with OCR. There is no private right of action, so complainants must depend on the government to ensure that the health care industry is abiding by the Privacy Rule. As shown above, relying on voluntary compliance is not an effective method of protecting our privacy rights.

2. Solution: Restructure the Privacy Rule

Voluntary compliance may be effective in some instances, but the Privacy Rule must be restructured to give OCR the discretion to impose fines without first seeking voluntary compliance.[123] For example, the Rule must allow for the immediate imposition of CMPs if, for example, the activity was egregious or repetitive. The Privacy Rule should provide a description of what is considered egregious or of how many violations constitutes repetitive behavior. By now OCR should have plenty of examples of what would be considered a particularly harmful or serious violation. OCR could establish standards and then issue guidelines about how it resolves different cases, including those that warrant the immediate imposition of CMPs.

As stated above, HHS does not disclose information about specific complaints, but one could imagine a situation in which a CMP

---

[122] 45 C.F.R. § 160.312 (2006).

[123] 45 C.F.R. § 160.312 (2006); Since writing this article, Senators Leahy and Kennedy introduced a bill that would permit the imposition of criminal and civil sanctions for unauthorized disclosures of personal health information without first seeking voluntary compliance. One of the purposes of the proposed legislation is to establish strong and effective remedies for violations of the law. *Health Information Privacy and Security Act,* S. 1814, 110th Cong. (2007). The bill, the Health Information Privacy and Security Act, was introduced in the Senate on July 18, 2007. *http://www.thomas.gov/cgi-bin/bdquery/z?d110:s.01814:* It was read twice and then referred to the Committee on Health, Education, Labor, and Pensions. *Id.* Since then, no major action has taken place. *Id.*

would be appropriate. For instance, consider the harm if everyone at a high school found out that a particular student was pregnant because a nurse at a hospital treated the student and then disclosed that information to her own teenage daughter who spread the information. This is a situation where the hospital should receive a CMP. The pregnant teenager has been harmed and there is no way to repair the injury. This is not a situation where voluntary compliance is appropriate. It would be unjust for OCR to consider the situation resolved if the hospital retrained the nurse or put a warning note in her employment file.

A CMP would also be suitable in a situation where prescription labels, pill bottles and computer printouts were found in a dumpster behind a pharmacy. The Health Privacy Project has reported several of these incidents.[124] Not only has this occurred repeatedly, but it is extremely careless. Pharmacies have the resources to properly dispose of customers' health information. This type of incident puts hundreds of consumers' health information in jeopardy and it would be unfair for OCR to allow these pharmacies to escape a penalty by simply issuing their employees a written warning.

Some may argue that actually imposing CMPs on covered entities would not be any more effective than voluntary compliance. Most covered entities are large corporations and a fine of even $25,000 per violation might seem inconsequential. Even so, if OCR started imposing CMPs, it would send a strong signal to the health care industry that the government is serious about enforcing the Privacy Rule.[125] The health care industry might finally believe that the Rule has "teeth." To combat this argument, the Rule could also be restructured to increase the maximum fine. Perhaps the Rule could allow for CMPs to be measured on a sliding scale, depending on the size of the covered entity, the seriousness of the violation, and the frequency of the violation.

Another related solution would be to restructure the Privacy Rule to allow OCR to fine the particular individual who violated the Privacy Rule rather than the covered entity employer. If a covered entity can prove that it has provided its staff with proper training and

---

[124] Health Privacy Project, *supra* note 105.

[125] "'The Securities and Exchange Commission, The Federal Trade Commission – they find significant and high-profile cases and send a message to the industry about what is permitted and what isn't,' said Peter Swire, an Ohio State University law professor who helped write the HIPAA regulations during the Clinton Administration." Stein, *supra* note 4.

has effective policies, procedures and systems in place, perhaps the rogue employee should be fined instead. This would provide individuals who work in the health care industry greater incentive to abide by the Privacy Rule. Many violations occur because people who work in a hospital or at a physician's office simply cannot contain their curiosity. For instance, many complainants have alleged that an employee of a covered entity accessed their medical records without permission and then spread their personal information. Covered entities can create safer and more secure systems to combat this problem, but often there is nothing that a covered entity could have done to prevent human faults. That is why, in certain circumstances, fining the individual would be more effective and fair than fining the covered entity.

Lastly, OCR could change its internal policy and reevaluate its "informal means" for resolving complaints. There may be instances where voluntary compliance is the proper course of action, but where the corrective action should be stronger. For instance, issuing a verbal or written warning to an employee might be sufficient in many situations, but retraining should never be allowed as mitigation. The Rule could enumerate exactly which enforcement activities are acceptable.

B. Proposal #2: Take the Privacy Rule Away From OCR

1. Problem: OCR is Incapable of Enforcing Laws

OCR is not properly enforcing the Privacy Rule, but that should come as no surprise. Historically, OCR has been notorious for its inability to effectively implement and enforce laws.[126] OCR is responsible for enforcing several laws in addition to the Privacy Rule, such as the nondiscrimination requirements of Title VI of the Civil Rights Act of 1964 ("Title VI"),[127] Sections 504 and 508 of the

---

[126] Vernellia Randall, *Eliminating Racial Discrimination in Health Care: A Call for State Health Care Anti-Discrimination Law,* 10 DEPAUL J. HEALTH CARE L. 1, 8 (2006)

[127] Title VI of the 1964 Civil Rights Act, Pub. L. No. 88-352, 78 Stat. 252 (1964), 45 C.F.R. § 80; Section 601 of Title VI provides: "No person in the United States, shall, on the grounds of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subject to discrimination under any program or activity receiving federal financial assistance.; HHS, OCR, *Civil Rights on the Basis of Race, Color, or National Origin, available at* http://www.hhs.gov/ocr/discrimrace.html (last visited March 15, 2007).

Rehabilitation Act of 1973, [128] Title II of the Americans with Disabilities Act of 1990 ("ADA"),[129] the Age Discrimination Act of 1975,[130] and the Hill-Burton Act.[131] Interestingly, each of these laws also has voluntary compliance provisions.

OCR has received the most criticism about its handling of Title VI, which protects people from discrimination based on their race, color, or national origin in programs or activities that receive federal financial assistance.[132] Almost all health care providers and institutions fall under OCR's Title VI jurisdiction, including hospitals, Medicaid and Medicare providers, physicians with patients assisted by Medicaid, Nursing Homes, and state agencies that are responsible for administering health care.[133] Unfortunately, as with HIPAA, private litigants have no right of action under Title VI,[134] which means that OCR is left with the sole responsibility for policing discrimination in health care.[135]

Scholars have suggested multiple reasons why OCR has been less aggressive in enforcing antidiscrimination laws in health than have civil rights agencies in other fields, such as employment and education.[136] One author proposed that "Congress designed OCR to be an impotent agency".[137] That assertion is difficult to dispute when, for instance, OCR has failed to collect racial and ethnic data from recipients of federal funds even though it is a requirement of Title

---

[128] The Rehabilitation Act of 1973, Pub. L. No. 93-112, as amended by the Rehabilitation Act Amendments of 1974, Pub. L. No. 93-516, 45 C.F.R. §§ 84-85; HHS, OCR, *Civil Rights on the Basis of Disability*, *available at* http://www.hhs.gov/ocr/discrimdisab.html (last visited March 15, 2007).

[129] Subtitle A of Title II of the Americans with Disabilities Act, Pub. L. No. 101-336, 28 C.F.R. § 35; *Id.*

[130] 45 C.F.R. § 91; HHS, OCR, *Other Civil Rights*, *available at* http://www.hhs.gov/ocr/discrimother.html (last visited March 15, 2007).

[131] 42 C.F.R. § 124; *Id.*

[132] 45 C.F.R. § 80. René Bowser, *Racial Profiling in Health Care: An Institutional Analysis of Medical Treatment Disparities*, 7 MICH. J. RACE & L. 79, 125 (2001). The poor enforcement history of Title VI naturally gives rise to pessimism regarding the prospects of attaining racial equality in health care through this legislation. *Id.*

[133] HHS, OCR, *Civil Rights on the Basis of Disability*, *available at* http://www.hhs.gov/ocr/discrimdisab.html (last visited March 15, 2007).

[134] *Alexander v. Sandoval*, 121 S. Ct. 1511 (2001); Christopher Bonastia, *The Historical Trajectory of Civil Rights Enforcement in Health Care*, 18 J. POL'Y HIST. 362, 364 (2006).

[135] Bonastia, *supra* note 134, at 365.

[136] *Id.*

[137] *Id.*

VI.[138] Other common complaints are that OCR has relied on individual complaints to enforce Title VI and that Title VI lacks specific definitions of prohibited discrimination and acceptable remedial action.[139] Sidney D. Watson, a professor at St. Louis University School of Law, has declared, "It is only when providers know that something is 'wrong' that they can be motivated to change the status quo to do what is 'right'."[140] Although these sentiments refer to Title VI and the debate about race and medical treatment, they echo much of what has been said about the Privacy Rule. OCR has proven over and over again that it is an incompetent agency.

2. Solution: Allow CMS to Enforce the Privacy Rule

OCR should be relieved of its duty.[141] The public would be better served if the government took the Privacy Rule enforcement authority away from OCR and gave it to a Federal agency that has had success with implementing and enforcing laws. The Centers for Medicare and Medicaid Services ("CMS") is a perfect candidate. CMS is responsible for the administration of Medicare, Medicaid, SCHIP (State Children's Health Insurance), the transaction and code set standards and the insurance portability requirements of HIPAA, and other health-related programs.[142] CMS has extensive experience deciding cases and enforcing laws.[143] In addition, CMS is already in

---

[138] Bonastia, *supra* note 134, at 376; Vernellia Randall, *Eliminating Racial Discrimination in Health Care: A Call for State Health Care Anti-Discrimination Law,* 10 DEPAUL J. HEALTH CARE L. 1, 15 (2006).

[139] Randall, *supra* note 138, at 15.

[140] René Bowser, *Eliminating Racial and Ethnic Disparities in Medical Care*, 30 ABA 24, 26 (2001).

[141] Bonastia, *supra* note 134, at 379. Civil rights responsibilities should be stripped from this "weak and dysfunctional agency." *Id.*

[142] CMS, *What is CMS?, at* http://www.cms.hhs.gov/home/tools.asp (follow "Frequently Asked Questions" hyperlink; then follow "What is CMS?" hyperlink) (last visited March 17, 2007); HHS Press Release, *CMS Named to Enforce HIPAA Transaction and Code Set Standards* (Oct 15, 2002), *available at* http://www.hipaacomply.com/CMS%20enforces%20Code%20Sets.htm.

[143] CMS, *Provider Reimbursement Review Board Decisions, available at* http://www.cms.hhs.gov/PRRBReview/PRRBD/list.asp (last visited March 21, 2007); CMS, *Decisions of the Medicare Geographic Classification Review Board , available at* http://www.cms.hhs.gov/MGCRB/03_MGCRB_Decision_Listings.asp#TopOfPage (last visited March 21, 2007); CMS, *Office of the Attorney Advisor, available at* http://www.cms.hhs.gov/OfficeAttorneyAdvisor/OAA/list.asp#TopOfPage (last visited March 21, 2007); CMS, *CMS Rulings, available at* http://www.cms.hhs.gov/Rulings/CMSR/list.asp#TopOfPage (last visited March 21, 2007).

charge of enforcing portions of HIPAA.[144] When former HHS Secretary Tommy G. Thompson announced that CMS would be responsible for enforcing part of HIPAA, he said "to accomplish this will require an enforcement operation that will assure compliance and provide support for those who file and process health care claims and other transactions [and] CMS is the agency best able to do this."[145] Clearly there would be an adjustment period, which would slow down the process for some time, but eventually CMS would be more efficient and fair at enforcing the Privacy Rule.

C. Proposal #3: Make Privacy Rule Complaints and Resolutions Available for Public Scrutiny

1. Problem: Privacy Rule Complaints and Resolutions are Kept Secret

Truth be told, nobody can accurately gauge whether OCR is effectively enforcing the Privacy Rule because everything is kept behind closed doors. It is virtually impossible to obtain copies of Privacy Rule complaints and closure letters, even in a redacted form.[146] These documents are not published. Purportedly, you can obtain copies of Federal Government records by making a Freedom of Information Act ("FOIA") request, but in reality the government is significantly backlogged and it is unclear how long the process takes.[147]

Without access to these records, public scrutiny of OCR's policies and processes is impossible. Congress is not even able to readily examine OCR's decisions. This seems to contradict the purpose of the Privacy Rule. The Rule is in place to protect the privacy of our personal health information, but what good is that when we are unable to monitor what complaints are made and how OCR resolves those complaints? How is the health care industry supposed to improve its privacy polices if these decisions are concealed? Currently, the Privacy Rule is being enforced in private. The government is abusing the Rule by preserving the confidentiality of its own actions. Perversely, the

---

[144] CMS, *at* http://www.cms.hhs.gov/ (last visited March 21, 2007).

[145] HHS Press Release, *supra* note 142.

[146] For purposes of this article, I submitted a FOIA request on November 17, 2006, and on December 8, 2007, I still did not know when I would receive copies of the closure letters I requested. I was told there is a significant backlog and that currently, FOIA requests take at least six months.

[147] The Freedom of Information Act, 5 U.S.C. § 552; HHS, *HHS Freedom of Information*, *at* http://www.hhs.gov/foia/ (last visited March 16, 2007).

current structure Privacy Rule enforcement protects the privacy of providers and regulators, rather than that of patients.

OCR may be the only federal agency that does not regularly publish its decisions. Federal agencies such as CMS, the U.S. Food and Drug Administration ("FDA"), and the Federal Trade Commission ("FTC") all publish opinions and decisions.[148] OCR has published a few of its Title VI decisions, but does not do so on a regular basis.[149] Administrative decisions are made public for a reason. Making this information available to everyone promotes consistency, provides transparency and increases public support and confidence in the system.[150]

2. Solution: Publish Privacy Rule Complaints and Closure Letters

OCR should publish the Privacy Rule complaints and closure letters.[151] This would allow the general public and the health care industry to review what violations are being alleged and how OCR resolves each case. Some may argue that these records contain personal information and should remain confidential. It is true these documents contain personal information, but a lot of personal information is published every day. Personal information is often included in administrative agency decisions and court opinions. Also, the government could easily publish this information using pseudonyms if necessary. There is no reason to hide the complainant's identity, but if a complainant wishes to remain anonymous, he or she

---

[148] Centers for Medicare and Medicaid Services, *at* www.cms.hhs.gov (last visited March 16, 2007); U.S. Food and Drug Administration, *at* www.fda.gov (last visited March 16, 2007); the Federal Trade Commission, *at* www.ftc.gov (last visited March 16, 2007).

[149] HHS, OCR, *Summary of Selected OCR Compliance Activities*, *available at* http://hhs.gov/ocr/mepa/complianceact.html (last visited March 21, 2007).

[150] Fredric Tulsky, *Ruling to Boost Court Scrutiny*, MERCURY NEWS, December 13, 2006, *available at* http://www.mercurynews.com/taintedtrials/ci_4832044; David Vladeck & Mitu Gulati, *Judicial Triage: Reflections on the Debate Over Unpublished Opinions*, 62 WASH. & LEE L. REV. 1667, 1676 (2005).

[151] Since writing this article, the Department of Health and Human Services, Office for Civil Rights, has added Privacy Rule case examples to its website. Please see: http://hhs.gov/ocr/privacy/enforcement/casebyissue.html#access (last visited January 19, 2007). Although this was a step in the right direction, it is still inadequate. The case examples are very brief and provide little information about the incidents or parties involved. Furthermore, the corrective actions taken are described in vague terms.

could opt for a pseudonym. Regardless of whether or not the complainant's identity is disclosed, this information should be made public so that we can truly critique the enforcement process.

V. CONCLUSION

The Privacy Rule is not working. Something must be changed to ensure that our personal health information is being protected and that the health care industry has an incentive to obey the law. For example, the government could restructure the Privacy Rule to give OCR real discretion to impose CMPs in appropriate circumstances, it could take the Privacy Rule enforcement power away from OCR and give it to another government agency, or it could start publishing Privacy Rule complaints and decisions. Voluntary compliance might seem like a fair policy, but it does not accomplish the primary purpose of the Privacy Rule, which is to provide consumers access to their health information and to control the inappropriate use of that information.[152] The Privacy Rule was enacted to sooth our fears and force the health care industry to follow specific standards, but so far it looks like the government has taken sides with the health care industry. The public will surely lose faith and trust in the system if it perceives that its "health information is not being carefully guarded or that privacy laws are not being enforced."[153]

[152] 65 Fed. Reg. 82,463 (Dec. 28, 2000).
[153] Sullivan, *supra* note 89.