Journal of Law and Health

Volume 17 | Issue 2 Article 6

2003

A Tripartite Threat to Medical Records Privacy: Technology, HIPAA's Privacy Rule and the USA Patriot

Nathan J. Wills

A TRIPARTITE THREAT TO MEDICAL RECORDS PRIVACY: TECHNOLOGY, HIPAA'S PRIVACY RULE AND THE USA PATRIOT ACT

I. INTRODUCTION

> "Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."[1] -Marlon Brando

[1] DAVID SHIPMAN, MARLON BRANDO (1974, revised 1989), *available at* http://www.bartleby.com/66/59/8159.html.

Virtually every member of American society has seen a physician and therefore has some type of medical history. A medical history contains some of the most intimate details of a person's life.[2] This information might not even be shared with intimate partners, family or friends,[3] perhaps because an individual is usually private, in denial of an illness, or wishes to guard loved ones from painful information. Whatever the reason, it is reasonable to conclude that most individuals wish to keep health information personal and private.

The desire to keep medical information private has been recognized for centuries, as evidenced by the Hippocratic Oath[4] and the common law physician-patient privilege.[5] As healthcare changes, so too must societal conceptions of medical privacy. Today, medical privacy encompasses not only privileged communications, but also the power to control medical records and who may access them. Preserving this power can appropriately be termed protecting medical records privacy.

Unfortunately, three issues threaten the long-recognized right to medical privacy. First, while the increased use of technology to store and transmit medical records makes accessing private health information easier for authorized medical personnel, it also increases the likelihood that the information may be seen and used by those with ill intentions. Second, the Privacy Rule promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[6] actually sanctions the non-consensual disclosure of personal health information.[7] Third, privacy rights are eroding as a result of measures taken to increase national security in the wake of the September 11, 2001 terrorist attacks. The erosion of privacy rights is illustrated by the hastily passed USA PATRIOT Act,[8] which alters the interpretation of many privacy oriented statutes and effectively contracts individual privacy rights.[9] These

---

[2]Kevin B. Davis, *Privacy Rights in Personal Information: HIPAA and the Privacy Gap Between Fundamental Privacy Rights and Medical Information*, 19 J. MARSHALL J. COMPUTER & INFO. L. 535, 537 (2001) (citing Board of Med. Quality Assurance v. Gherardini, 93 Cal. App. 3d 669, 678 (1979)).

[3]Peter P. Swire & Lauren B. Steinfield, *Modern Studies in Privacy Law: National Health Information Privacy Regulations Under HIPAA: Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1526-27 (2002).

[4]STEDMAN'S MEDICAL DICTIONARY 799, *cited in* Mike Hatch, *Modern Studies in Privacy Law: National Health Information Privacy Regulations Under HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1489 (2002).

[5]Lawrence O. Gostin and James G. Hodge, Jr., *Piercing the Veil of Secrecy in HIV: AIDS and Other Sexually Transmitted Diseases: Theories or Privacy and Disclosure in Partner Notification*, 5 DUKE J. GENDER L. & POL'Y 9, 42 – 44 (1998).

[6]Pub. L. No. 104-191 (1996) (codified as 42 U.S.C. § 201).

[7]Compliance with the Privacy Rule is required no later than April 14, 2003 for "covered entities" except "small health plans." "Small health plans" must comply with the Rule by April 14, 2004. 45 C.F.R. §164.534. *See also* 65 Fed. Reg. 82,462. A "small health plan" has annual receipts of less than $5 million. 45 C.F.R. §160.104.

[8]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Act of 2001) (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

[9]Swire & Steinfield, *supra* note 3, at 1521-22.

three factors have converged to threaten an individual's right to medical records privacy.

Proceeding from the proposition that privacy is a fundamental right, this essay notes the importance of maintaining medical records privacy in light of the increased use of technology. It describes the Privacy Rule promulgated under HIPAA, which was intended to strengthen medical records privacy, but notes the restriction of privacy rights following September 11, 2001 ("9/11"). In light of circumscribed privacy rights, the Privacy Rule becomes much more important in protecting medical records privacy. Unfortunately, the Rule falls short of this goal by potentially running afoul of the First and Fourth Amendments. It also fails to provide adequate medical records protection because it: (1) relies on an out of date technology model; (2) provides too many exceptions to its own consensual disclosure provisions; (3) lacks specificity in defining the entities it covers; (4) fails to resolve important federalism issues; and (5) caters to corporate interests. These problems can be corrected by bolstering computer security, changing the text of the Rule to anchor a patient's "reasonable expectation of privacy," and offering the judiciary an avenue to continue to expand privacy rights despite the nation's post-9/11 fears.

II. PRIVACY IS A FUNDAMENTAL RIGHT

> "[T]he makers of our Constitution conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men."[10] -Justice Louis Brandeis

While the Constitution does not explicitly grant the right to privacy, the United States Supreme Court has recognized this guarantee.[11] One of the earliest recognitions of the right to privacy came in the 1891 decision of *Union Pacific Railway v. Botsford*.[12] Finding that an injured woman could not be required to submit to a surgical examination to determine the extent of her injuries, the Supreme Court noted that "[n]o right is held more sacred, or is more carefully guarded . . . than the right of every individual to the possession and control of his own person, free from all restraint or interference of others . . . ."[13]

The 1928 decision of *Olmstead v. United States* formally tied privacy rights to the Fourth Amendment protection against unreasonable searches and seizures.[14] Justice Brandeis noted in his dissent that the drafters of the Constitution, in an effort to allow for the pursuit of happiness and to protect the beliefs of Americans, "conferred, as against the government, the right to be let alone."[15] That right, he asserted, was promulgated in the text of the Fourth Amendment.[16] Similarly, in the

---

[10]Olmstead v. United States, 277 U.S. 438, 478 (1928).

[11]James G. Hodge, Jr., *National Health Information Privacy and New Federalism*, 14 ND J. L. ETHICS & PUB. POL'Y. 791, 797 (2000).

[12]141 U.S. 250, 251 (1891).

[13]*Id.*

[14]*Olmstead*, 277 U.S. at 478.

[15]*Id.*

[16]*Id.*

1965 decision of *Griswold v. Connecticut*, Justice Douglas noted that the penumbral zones of privacy stem from the emanations of the Fourth Amendment "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[17] In light of these decisions, privacy may appropriately be regarded as a fundamental right with a substantial historic pedigree.

Unfortunately, the right to privacy is limited and poorly defined because it emanates from the penumbras of the Fourth Amendment, and is therefore easily subject to transgression.[18] The right faces further limitation from other social interests, such as the need for openness and transparency or other compelling State interests, which are often balanced against it.[19]

Ferguson v. City of Charleston recently addressed the balance between medical privacy and State interests.[20] In response to the increased use of cocaine by expectant mothers, The Medical University of South Carolina ("MUSC") began screening urine samples of maternity patients suspected of drug use.[21] Under MUSC policy, if a patient tested positive for cocaine use during labor or a prenatal care visit, medical staff threatened to report the patient's drug use to law enforcement officials.[22] The patient could avoid criminal sanctions by enrolling in a substance abuse program.[23]

The Supreme Court found for the Plaintiffs, stating that MUSC had violated the Fourth Amendment protection against unreasonable search and seizure.[24] In deciding the case the Court noted that MUSC was subject to the Fourth Amendment because it was a state hospital.[25] It also identified the well-settled principle of law that urine tests are considered searches under the Fourth Amendment.[26] Balancing the patients' Fourth Amendment privacy interests against the "special needs" of the hospital, the Court concluded that the tests were an unreasonable search in violation of the Fourth Amendment.[27] The Court also noted that a patient's "reasonable

---

[17]Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[18]Kevin B. Davis, *Privacy Rights in Personal Information: HIPAA and the Privacy Gap Between Fundamental Privacy Rights and Medical Information*, 19 J. MARSHALL J. COMPUTER & INFO. L. 535, 538 (Summer 2001).

[19]Marc Rotenberg, *Modern Studies in Privacy Law: Foreward: Privacy and Secrecy After September 11*, 86 MINN. L. REV. 1115, 1127 (June 2002).

[20]532 U.S. 67 (2001).

[21]Samples were screened if a patient met one or more of the following criteria: (1) no prenatal care; (2) late prenatal care after 24 weeks gestation; (3) incomplete prenatal care; (4) abruptio placentae; (5) intrauterine fetal death; (6) preterm labor 'of no obvious cause'; (7) IUGR (intrauterine growth retardation) 'of no obvious cause;' (8) previously known drug or alcohol abuse; and (9) unexplained congenital anomalies. *Id.* at 72.

[22]*Ferguson* at 72.

[23]*Id.*

[24]*Id.* at 85.

[25]*Id.* at 76.

[26]*Ferguson* at 76.

expectation of privacy" is that the results of diagnostic tests will not be shared with non-medical personnel without her consent.[28]

While privacy rights prevailed in *Ferguson*, the balancing test employed illustrates that the extent of privacy rights may not be well-settled. Nevertheless, previous Supreme Court decisions indicate that privacy may appropriately be regarded as a fundamental right.[29] This treatment is justified; for without privacy an individual's medical records might be used to deny credit, employment, or insurance coverage.[30] Similarly, without privacy rights a person would be subject to being embarrassed by neighbors and stigmatized or humiliated by friends and relatives.[31] The right to privacy is therefore co-extensive with protecting individual dignity and fulfills an essential role of individual autonomy and a free society.[32] To protect individual dignity, preserve personal security and allow for the pursuit of happiness, privacy must encompass not only 'the right to be let alone,' but also the right to control the release of personal and private information.[33]

III. MEDICAL RECORDS PRIVACY IS OF THE UTMOST IMPORTANCE

> "All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."[34]
>
> -The Hippocratic Oath

The right to privacy is of paramount importance in the medical records context because medical records contain highly sensitive information about what are potentially the most intimate details of an individual's life.[35] Medical records often contain demographic information such as age, sex, race, marital status, children, and occupation; financial information, such as employment status, income, and methods of payment; personal identifiers other than name, including social security number, addresses, and phone numbers; and information about why treatment is sought, such as being the victim of a violent crime, firearm injury, or the at-fault party in an auto accident.[36] They also contain information identifying whether an individual has a

---

[27]The "special needs" asserted by the state were its' interest in curtailing the pregnancy costs and medical complications resulting from maternal cocaine use. *Ferguson* at 78.

[28]*Ferguson* at 78.

[29]Mike Hatch, *Modern Studies in Privacy Law: National Health Information Privacy Regulations Under HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1487 (2002).

[30]*Id.*

[31]*Id.* at 1486.

[32]*Id*.

[33]Samuel D. Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

[34]STEDMAN'S MEDICAL DICTIONARY 799, *cited in* Hatch, *supra* note 29, at 1489.

[35]Davis, *supra* note 18, at 537.

[36]Hodge, *supra* note 11, at 791.

communicable or other disease, or a particular genetic propensity.[37] When aggregated, this information reveals a great deal about the intimate details of a person's life.[38] It also creates a profile of a person that may be used for discriminatory purposes such as denying credit, employment, or insurance coverage.[39]

Changes in the healthcare industry have coalesced to de-emphasize medical records security and make health information a commodity. As medical records are increasingly stored and transmitted in electronic media[40] unauthorized disclosures or security breaches have become more frequent.[41] The centralized storage of medical records also allows individuals to be identified in reverse.[42] By searching based on diseases rather than names, it is possible to create lists of people with specific medical conditions.[43] Employers with access to health identifiers and database information can use these lists to wrongfully discriminate and deny jobs based on the projected cost of a pre-existing medical condition to the company's health plan.[44] Participants in the healthcare industry may also use this information to learn about individuals who use their products or are affected by a particular medical condition.[45] They may then use this information in unsolicited marketing efforts.[46]

Consider too the number of people who potentially see part or all of a patient's medical record during a typical hospital stay. Once a patient is admitted to a hospital, information is gathered and disseminated to a multitude of entities,[47] including regulatory agencies, accreditation bodies, government departments, insurance providers, data warehouse and storage facilities, researchers, billing and accounting, third party benefit managers, marketers, insurers, and in some cases, even employers.[48] This is to say nothing of the multitude of healthcare employees who view an individual's personal health information in the course of treatment, or

---

[37]*Id.*

[38]Jerry Berman, *The Federal Trade Commission's Report to Congress- 'Privacy Online: Fair Information Practices in the Electronic Marketplace*,' testimony before the Senate Committee on Commerce, Science and Transportation, May 25, 2000, *available at* www.cdt.org/testimony/000525berman.shtml (last visited Feb. 17, 2002, on file with author).

[39]Hatch, *supra* note 29, at 1490.

[40]Davis, *supra* note 18, at 539.

[41]Hatch, *supra* note 29, 1491.

[42]Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J. LAW & TEC. 319, 358 (Spring 2002).

[43]*Id.*

[44]*Id.*

[45]Davis, *supra* note 18, at 539.

[46]*Id.*

[47]Charity Scott, *Is Too Much Privacy Bad For Your Health?: A Introduction to the Law, Ethics, and HIPAA Rule On Medical Privacy*, 17 GA. ST. U. L. REV. 481, 484 (2000).

[48]Davis, *supra* note 18, at 544-45. The HHS regulations prohibit the use of health information by employers for job related decisions.

the ease of access to computer terminals within the hospital setting. By some estimates, over four hundred people are likely to see part or all of a patient's medical record during a typical hospital stay.[49]

The decrease in medical records privacy creates not only the potential for unwarranted and possibly illegal misuse or discrimination by healthcare providers, insurance companies, employers and marketplace participants; it may also adversely affect the quality of care. A 1999 survey conducted by the California HealthCare Foundation indicated that the public has reacted to the perceived decrease in medical records privacy by engaging in privacy-protective behavior to shield themselves from harmful and intrusive uses of health information.[50] This behavior included withholding information from healthcare providers, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out-of-pocket for care that is covered by insurance and, in the most extreme cases, avoiding care altogether.[51] The survey also showed that one in five persons believe that their personal health information had been compromised and used inappropriately, and that one in six engaged in some form of the previously described privacy protective conduct.[52] Similarly, a Harris Equifax survey showed that over 80% of the public respondents felt they had "lost all control" over their personal information.[53] "This has led some members of the health care industry to state that medical record privacy is not just failing, it is 'non-existent.'"[54]

IV. HIPAA: THE GOVERNMENT'S RESPONSE TO THREATENED MEDICAL RECORDS PRIVACY

> "Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[55] -Justice Louis Brandeis

Congress passed the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to promote the use of technology in the medical field and to standardize

---

[49]Davis, *supra* note 18, at 544.

[50]California HealthCare Foundation, National Survey: Confidentiality of Medical Records (Oakland: CHCF, Jan. 1999), *cited in* Janlori Goldman and Zoe Hudson, *Virtually Exposed: Privacy and E-Health; Privacy concerns are keeping consumers from reaping the full benefit of online health information*, HEALTH AFFAIRS, Nov/Dec 2000.

[51]*Id*.

[52]*Id*.

[53]Lawrence O. Gostin, James G. Hodge, Jr. and Mira S. Burghardt, *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule*, 46 ST. LOUIS J.L. 5, 6 (Winter 2002).

[54]Davis, *supra* note 18, at 544.

[55]*Olmstead*, 277 U.S. at 479.

and streamline medical records.[56] The proposed changes were designed to improve patient care, ameliorate the healthcare system's administrative inefficiencies, and decrease costs through the free flow of information.[57] These "administrative simplification" provisions included the creation of a Uniform Health Identifier (UHID) and a "national electronic collection system for personal health care data."[58]

Recognizing that free flowing medical information and a UHID would reduce privacy by making information available to those who could access the records storage system, Congress required that medical records privacy legislation be passed by August 21, 1999.[59] Congress failed to pass that legislation and, pursuant to the HIPAA mandate, the Secretary of the Department of Health and Human Services ("HHS") was authorized to pass privacy regulations.[60]

HHS issued a proposed Privacy Rule in November of 1999, at which time over 50,000 public comments were received.[61] These comments reflected concern over the impact of the Rule on the healthcare industry, illustrated confusion and misunderstanding over how it would operate, and expressed apprehension about its complexity.[62] Several thousand additional comments were received when President Bush re-opened the comment period in efforts to re-assess regulations enacted late in former-President Clinton's term.[63] Despite the concerns enunciated in the comments, President Bush announced in April of 2001 that the Privacy Rule would go into effect essentially as drafted, requiring compliance after April 2003.[64]

---

[56]Rob Cunningham, *Old Before Its Time: HIPAA and E-Health Policy; A Law that Predates the Internet Explosion Needs Retrofitting to Serve as a Foundation for Standardized Data Exchange*, HEALTH AFFAIRS, Nov/Dec 2000.

[57]*Id.* *See also* Standards for Privacy of Individually Identifable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000); Andrew S. Krulwich and Bruce L. McDonald, *The Vulnerability of HIPAA Regulations to First and Fourth Amendment Attack: An Addendum to "Evolving Constitutional Privacy Doctrines Affecting Healthcare Enterprises,"* 56 FOOD DRUG L.J. 281, 282-83 (2001).

[58]Sobel, *supra* note 42, at 325. While the idea of a UHID has "acquired the aura of a third rail," it indicates that if the administrative simplification provisions "are not refashioned, federal policy will fall further behind events." Off-the-record interview with HHS official, June 20, 2000 *cited in* Cunningham, *supra* note 56.

[59]Gostin et al., *supra* note 53, at 15.

[60]HIPAA, Pub. L. No. 104-191, 264(c)(1) (1996), *cited in* Gostin et al., *supra* note 53, at 15.

[61]Press Release, U.S. Department of Health and Human Services, *Protecting the Privacy of Patients' Health Information* (May 9, 2001), *available at* http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm (last visited Nov. 21, 2003, on file with author), *cited in* Gostin et al., *supra* note 55, at 15.

[62]Standards for Privacy of Individually Identifable Health Information, 67 Fed. Reg. at 53182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160 & 164).

[63]Robert Pear, *Bush Accepts Rules to Protect Privacy of Medical Records*, N.Y. TIMES, Apr. 12, 2001, at A1, *cited in* Gostin et al., *supra* note 53, at 15, n.53.

[64]Swire & Steinfeld, *supra* note 3, at 1524.

The Privacy Rule begins by defining "health information,"[65] then explicitly governs a subset of that information known as "protected health information" ("PHI").[66] PHI includes individually identifiable information transmitted and maintained electronically or in any other form or media.[67] This includes, for example, information containing a name, Social Security Number, driver's license number, fingerprint, or genetic link.[68] The information may be categorized as "de-identified" and no longer subject to the Rule upon finding a "very small" risk of subject identification or upon removal of a specified list of identifiers.[69] Also, truly non-identifiable information is not subject to the Rule because there are no privacy implications.[70]

The Privacy Rule applies only to "covered entities," defined as health care providers, health plans, and healthcare clearinghouses.[71] The Rule requires, *inter alia*, that they provide notice of their information practices,[72] use and disclose PHI only with patient permission except in cases of designated exceptions,[73] permit patients to access and request correction of their records,[74] and provide patients an accounting of PHI disclosure.[75] "Covered entities" must also limit the use and disclosure of PHI to the minimum necessary amount,[76] implement security

---

[65]Public Welfare General Administrative Requirements, 45 C.F.R. § 160.103 (2003). Health information means any information, whether written or 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.

[66]*Id.*

[67]*Id.*

[68]Public Welfare Security and Privacy, 45 C.F.R. § 164.514(b)(2)(i) (2003).

[69]45 C.F.R. § 164.514(b). These identifiers include names, geographic subdivisions smaller than a State, all elements of dates relating to an individual (e.g. those that indicate the patient's age), telephone numbers, fax numbers, e-mail addresses, Social Security Numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate or license numbers, vehicle identifiers, device identifiers, URLs, IP (Internet Provider) address numbers, biometric identifiers such as finger and voice prints, full face photographic images, and any other unique identifying number, characteristic or code, *supra*.

[70]Gostin et al., *supra* note 53, at 17-18.

[71]45 C.F.R. § 160.103(3).

[72]45 C.F.R. § 164.520(a)(1).

[73]45 C.F.R. § 164.512.

[74]45 C.F.R. § 164.526(a).

[75]45 C.F.R. § 164.528(a)(1).

[76][A] covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. 45 C.F.R. § 164.502(b)(1).

safeguards to protect against unauthorized access or disclosure,[77] and obtain satisfactory assurances, via a written contract, that their business associates using PHI protect the privacy of the information.[78]

The Rule was intended to enhance patient autonomy and promote trust in the health care system.[79] It ostensibly increases the accountability of "covered entities" by allowing patients to access certain information contained in their files and by regulating the covered entities' use of PHI.[80] It should also bridge the gap between the privacy interests articulated by the Supreme Court and the personal health information that people might choose to keep out of the public domain.[81]

Critics however, have described the Privacy Rule as a "regulatory oxymoron."[82] While intended to protect the privacy of personal health information, the Rule actually sanctions non-consensual disclosure in certain instances.[83] For instance, PHI may be disclosed without patient consent: to public health authorities to prevent or control disease or to report child abuse or neglect;[84] to the Food and Drug Administration (FDA) to report "adverse events" and biological product deviations, to track products, or to conduct post marketing surveillance;[85] to a person who may have been exposed to a communicable disease or who is at risk of spreading the disease;[86] and to employers regarding evaluation of the workplace, a work related illness, or workplace medical surveillance.[87] The Rule also allows nonconsensual disclosure of PHI about victims of abuse, neglect or domestic violence,[88] or for oversight of the healthcare system, government benefit programs, entities subject to government regulatory programs, or entities subject to civil rights laws.[89] Because the Privacy Rule sanctions the non-consensual disclosure of PHI, it may appropriately be viewed as a threat to medical records privacy.

---

[77]45 C.F.R. § 164.530(c)(2).

[78]45 C.F.R. § 164.502(e)(2).

[79]Gostin et al., *supra* note 53, at 21.

[80]Davis, *supra* note 18, at 537.

[81]*Id.*

[82]Hatch, *supra* note 29, at 1483.

[83]*Id*.

[84]45 C.F.R. § 164.512(b)(1)(i) & (ii).

[85]45 C.F.R. § 164.512(b)(1)(iii).

[86]45 C.F.R. § 164.512(b)(1)(iv).

[87]45 C.F.R. § 164.512(b)(1)(v).

[88]*Id*.

[89]45 C.F.R. § 164.512(d)(1).

V. PRIVACY RIGHTS ARE CIRCUMSCRIBED IN THE POST-9/11 WORLD

> "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[90] -Benjamin Franklin

The United States Supreme Court had been expanding privacy rights prior to the terrorist attacks of September 11, 2001, but the penumbral zones of privacy constricted following those tragic events.[91] For example, privacy rights prevailed in the pre-9/11 *Ferguson* case as the Court noted that a patient has a reasonable expectation that the results of diagnostic tests will not be disclosed to non-medical personnel without patient consent.[92] Similarly, in *Kyllo v. United States* the Court found that law enforcement's use of thermal-imaging to scan an individual's home violated the Fourth Amendment protection against unreasonable searches and seizures.[93] Public opinion prior to 9/11 also supported expanded privacy rights, as a Wall Street Journal poll found that Americans ranked the "erosion of personal privacy" as one of the most serious issues in the upcoming century.[94]

Following 9/11, priorities clearly changed, as security issues moved to the fore of the public mind.[95] Post-9/11 polls indicating greater concern for public safety and a noticeably lower concern for privacy issues illustrate this change.[96] Public opinion increasingly supported new forms of surveillance, including biometric identifiers[97] and a national ID card.[98] Concomitantly, the momentum towards increasing individual privacy quickly shifted towards protecting national security through greater surveillance powers than would have been proposed only a year earlier.[99]

The passage of the USA Patriot Act exemplifies the declining importance of individual privacy. Its provisions grant broad and often unchecked discretion to law enforcement officials. For example, rather than requiring a new search warrant for each phone or computer, law enforcement officials may now access communications from any device used by a suspect.[100] Similarly, the Act increases the scope of

---

[90]HISTORICAL REVIEW OF PENNSYLVANIA, *available at* http://www.bartleby.com/100/245.1.html#245.note2 (last visited Feb. 17, 2003).

[91]Andrew S. Krulwich and Bruce L. McDonald, *The Vulnerability of HIPAA Regulations to First and Fourth Amendment Attack: An Addendum to "Evolving Constitutional Privacy Doctrines Affecting Healthcare Enterprises,"* 56 FOOD DRUG L.J. 281, 303 (2001).

[92]Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

[93]Kyllo v. United States, 533 U.S. 27 (2001).

[94]Swire & Steinfeld, *supra* note 3, at 1515.

[95]*Id*.

[96]*Id*. at 1515-16.

[97]Examples of biometric identifiers include finger and voice prints. *See*, 45 C.F.R. §164.514(b)(2)(i)(P).

[98]Rotenberg, *supra* note 19, at 1115.

[99]Swire & Steinfeld, *supra* note 3, at 1516.

[100]This power is referred to as a "roving wire-tap." *See*, Swire & Steinfeld, *supra* note 3, at 1521.

emergency orders used to trace communications,[101] which generally apply before a judge approves a court order.[102] The Act also provides that one court order may be used for tracing communications nationwide, rather than requiring a new order in each jurisdiction a communications provider operates.[103]

The USA PATRIOT Act also changes the interpretation of many privacy oriented statutes, which effectively restricts individual privacy rights.[104] Information developed under the Foreign Intelligence Surveillance Act may now be used in a wider range of cases.[105] Similarly, suspects will no longer be informed that they were under surveillance, even after the fact.[106] Information developed by a grand jury may now be shared with intelligence agencies,[107] and law enforcement officials are permitted to set up extended residence at a communications provider to monitor the communications of unauthorized users.[108] This latter expansion of power was never even the subject of a Congressional hearing.[109] The FBI may also review sensitive personal information, including medical, financial, mental health, and educational records, without having to show evidence of a crime and without a court order.[110]

While the intent of the USA PATRIOT Act was to reduce the threat of future terrorist attacks by increasing national security, it also has the effect of significantly weakening the structure and limiting the coverage of many privacy protection statutes.[111] Not only can the government use its expanded powers to combat terrorism, it can also use these powers against American citizens who are not under criminal investigation; against immigrants, who are within American borders legally; and against all those whose First Amendment activities are deemed to be national security threats by the Attorney General.[112] Indeed, non-terrorist suspects are now subject to the government's expanded ability to conduct secret searches in routine investigations wholly unrelated to terrorism.[113]

---

[101]107 Pub. L. 56 at 212.

[102]*Id*. at 213.

[103]*Id*. at 220.

[104]Swire & Steinfield, *supra* note 3, at 20-21.

[105]107 Pub. L. 56 at 215.

[106]*Id*. at 214.

[107]*Id*. at 215.

[108]*Id*. at 216.

[109]107 Pub. L. 56 at 216. Swire, *supra* note 3, at 1521-22.

[110]Sobel, *supra* note 42, at 376.

[111]Rotenberg, *supra* note 19, at 1118.

[112]Stephanie Olsen, *Patriot Act Draws Privacy Concerns*, CNETNews.com (Oct. 26, 2001), available at, http://news.com.com/2100-1023-275026.html?tag=prntfr, *quoting*, Gregory T. Nojeim, of the ACLU's Washington Office (last visited, Feb. 17, 2003, on file with author).

[113]Sobel, *supra* note 42, at 376.

The passage of the USA PATRIOT Act evidences the circumscription of privacy rights following 9/11. It has been described as the most sweeping expansion of government surveillance since the passage of the Communications Assistance for Law Enforcement Act of 1994.[114] Similarly, the ACLU noted that "the USA PATRIOT Act gives enormous, unwarranted power to the executive branch unchecked by meaningful judicial review."[115] These changes have effectively increased the power of the government by reducing an individual's protection against unwanted governmental intrusion into their personal lives. [116]

VI. THE THREAT TO MEDICAL RECORDS PRIVACY

> "The experience of democracy is like the experience of life itself - always changing, infinite in its variety, sometimes turbulent and all the more valuable for having been tested by adversity."[117] -Jimmy Carter

The three issues described above have converged to threaten medical records privacy. First, the increased use of technology creates greater possibility for unauthorized access to personal health information. Healthcare providers, insurance companies, employers and marketplace participants can use this information for discriminatory purposes.[118] Second, the Privacy Rule, which was promulgated in an effort to address this threat, falls short of its goal because it sanctions the non-consensual disclosure of personal health information.[119] Third, privacy rights are further threatened by their severe restriction in the wake of the September 11 terrorist attacks, as evidenced by the passage of the USA PATRIOT Act.[120]

The intersection of these events illustrates the tension between preserving individual privacy rights and protecting national security. On one hand, legislators and the judiciary attempted to strengthen medical records privacy rights by passing the Privacy Rule. On the other, the threat of terrorism dictated that national security be given greater priority. Increased security has had the unfortunate by-product however, of decreasing individual privacy rights. Because these opposing interests threaten medical records privacy, the proposed Privacy Rule must now be scrutinized, and in some cases reworked, to create meaningful privacy protections. Accordingly, this essay reconsiders the efficacy of the Privacy Rule in light of circumscribed and contracting privacy rights.

---

[114]Rotenberg, *supra* note 21 at 1116. *See* Communications Assistance for Law Enforcement Act of 1994, 103 Pub. L. No. 414 (codified at 47 U.S.C. 1001-1010 (1995)).

[115]Sobel, *supra* note 42, at 376-77.

[116]Rotenberg, *supra* note 19, at 1132-33.

[117]Address to Indian Parliament Jan. 2, 1978 *available at* http://www.bartleby.com/63/26/26.html (last visited Feb. 17, 2003, on file with author).

[118]Davis, *supra* note 18, at 539-40.

[119]Hatch, *supra* note 29, at 1483.

[120]Rotenberg, *supra* note 19, at 1118.

VII. CRITICISM OF THE PRIVACY RULE

"Lawyers come forward when there are great challenges."[121]
-Alexis de Tocqueville

A. Is the Privacy Rule Unconstitutional?

There is substantial justification for the argument that the Privacy Rule is unconstitutional under the Fourth and First Amendments.[122] While this argument has never been adjudicated in court, it was presented in *The Association of American Physicians & Surgeons, Inc. v. United States Department of Health and Human Services*.[123] The case was ultimately dismissed for lack of standing by the United States District for the Southern District of Texas, Houston Division, but the arguments presented illustrate the Privacy Rule's susceptibility to a Constitutional challenge.

1. Fourth Amendment Claims

Plaintiffs, The Association of American Physicians & Surgeons, Inc., a Congressman, and three patients argued that the Privacy Rule violated the Fourth Amendment prohibition against unreasonable government searches and seizures.[124] Plaintiffs alleged that the Rule violates the Fourth Amendment by: (1) giving the government virtually unrestricted access to medical records without a warrant; (2) requiring that physicians aid government searches of patient records; and (3) facilitating the construction of a centralized government database of PHI without patient consent.[125]

In disposing of the case the court found that "a number of unlikely events must occur in order for plaintiffs to sustain an injury."[126] The Secretary of HHS would have had to exercise his oversight responsibility under 45 C.F.R. §160.310(c) to request access to PHI, and would then have had to proceed directly against the "covered entity" that possessed the PHI in question.[127] Even then, Plaintiffs' particular PHI might not even have been accessed.[128]

---

[121]DEMOCRACY IN AMERICA, 290 (Random House 1945) (1835), *cited in*, Rotenberg, *supra* note 19, at 1135.

[122]*See e.g.*, The Association of Am. Physicians & Surgeons, Inc. et al. v. United States Dep't of Health and Human Services et al., 224 F. Supp. 2d 1115 (2002). *See also*, Krulwich, *supra* note 91, at 303.

[123]224 F. Supp. 2d 1115 (2002).

[124]*Id.* at 1120.

[125]*Id.* at 1120-21.

[126]*Id.* at 1123.

[127]*Id.* 45 C.F.R. §160.310(c) states in pertinent part "A covered entity must permit access by the Secretary [to its sources of information] that are pertinent to ascertaining compliance with the applicable requirements [and standards]."

[128]*Association of Am. Physicians*, 224 F. Supp. 2d at 1123.

As Plaintiffs' PHI was not directly threatened, the Court concluded that Plaintiffs' allegations against HHS were "highly speculative"[129] and that Plaintiffs had neither established ripeness nor standing.[130] Moreover, Plaintiffs failed to establish that the Privacy Rule had any immediate impact on them, that a legally protected interest had been invaded, or that they would suffer hardship resulting from the court's failure to consider their claims.[131]

The speculative nature of Plaintiffs' injury however, is unique to the *Association of American Physicians & Surgeons* case. As a counter-example, in *Ferguson v. City of Charleston*, *infra*, MUSC violated the Fourth Amendment by disclosing the results of diagnostic tests to local law enforcement without patient consent or a warrant.[132] Under the current draft of the Privacy Rule, this same information could now be lawfully disclosed under the Rule's provisions to prevent disease or child abuse.[133] Similarly, if Plaintiff's diagnostic test results had been transmitted electronically, the information would be subject to the USA PATRIOT Act, and could be accessed by the FBI without a court order under its authority to review medical information. [134]

These scenarios illustrate how the intersection of technology, the Privacy Rule and the USA PATRIOT Act abrogate privacy rights and violate the Fourth Amendment. Ironically, information that was constitutionally protected before the promulgation of the Privacy Rule would be subject to non-consensual disclosure under a law designed specifically to increase privacy. Clearly, there are situations where an application of the Privacy Rule would violate the Fourth Amendment prohibition against unreasonable searches, and where an injury under the Rule would not be speculative. When the USA PATRIOT Act is added to the equation, the threat to medical records privacy becomes glaringly apparent.

2. First Amendment Claims

Plaintiffs in *Association of American Physicians & Surgeons* also alleged that the Privacy Rule violated their First Amendment right to free speech.[135] They argued that speech between patients and physicians was chilled by the mere existence of the Rule because patients were reluctant to speak freely with their physician.[136] These allegations were dismissed as the Court found that they were subjective, and therefore non-actionable, and that Plaintiffs' alleged injury could not be redressed by a favorable court decision.[137]

---

[129]*Id.*

[130]*Id.*

[131]*Id.* at 1124.

[132]*Ferguson v. City of Charleston*, 532 U.S. 67 (2001).

[133]45 C.F.R. §164.512(b)(i) and (ii).

[134]Sobel, *supra* note 42, at 1125.

[135]*Association of Am. Physicians*, at *20-21.

[136]*Id.*

[137]*Id.*

Ferguson provides an example of how an application of the Privacy Rule would violate the First Amendment right to free speech. If Plaintiffs in *Ferguson* had failed to disclose their cocaine use to their physicians for fear that the information would be reported to government officials under the Rule's child abuse provisions, Plaintiffs' speech would have been chilled.[138] This chilling effect would constitute an injury to Plaintiffs as a direct result of an application of the Privacy Rule because Plaintiffs would have failed to speak due to a fear of disclosure under the Rule. Similarly, if Plaintiffs' failure to disclose their addiction harmed the child and the harm could have been prevented by full disclosure, Plaintiffs would have been injured by an application of the Rule. Finally, had Plaintiffs disclosed their cocaine addiction with the understanding that those communications were confidential, and Plaintiffs were subsequently arrested on the grounds of that communication and the urine test that followed, Plaintiffs would have been injured by an application of the Rule. In these scenarios, a patient would be injured under the application of the Privacy Rule, which was promulgated in order to protect patient privacy.

B. If not Unconstitutional, the Privacy Rule is Ineffective

While finding the Privacy Rule unconstitutional might require an unusual confluence of factors, it is nevertheless ineffective in achieving substantial medical records privacy. First, the rate of technological change renders many of the Rule's provisions obsolete.[139] Second, the exceptions to the consent provisions subsume much of the privacy protection that might have otherwise been gained. Third, the definition of a "covered entity" is so ambiguous that entities might deal with PHI but fall outside of the definition, and therefore not be subject to the Rule. This ambiguity is of particular concern to consumers who might inadvertently disclose information under the mistaken belief that an entity is covered, when in fact it is not. Fourth, the Rule presents federalism questions that must be addressed because individual privacy has traditionally been a state function and the Privacy Rule is a federal regulation. Finally, the government's goal in passing the Privacy Rule was never to protect individual privacy rights. Rather, Congress wanted to increase the portability of health information, thereby furthering corporate interests instead of protecting citizens against privacy violations. The Privacy Rule was an afterthought included to more effectively market the mobility of health information. Accordingly, while Congress recognized that privacy provisions were required to make medical records standardization palatable, it did not go far enough.

1. The Privacy Rule Is Behind the Times

The Privacy Rule fails to address contemporary medical records storage and transmission practices because it was based on an outdated technology model. The Rule was promulgated under the technology model of the mid-1990s when electronic health information was stored in large, centralized payer and provider systems.[140] Technological changes now allow that information to be stored in a common cyber-space supported by Internet Service Providers (ISP's) and accessed by Web

---

[138]45 C.F.R. §164.512(b)(i) and (ii).

[139]Cunningham, *supra* note 56, at 231.

[140]*Id.*, Off-the-record interview with HHS official (June 9, 2000).

browsers.[141] These changes facilitate the storage and transmission of vast amounts of data, but allow that same information to be accessed by anyone with a modem and a PC.[142]

Similarly, the Privacy Rule fails to account for the prevalence of Internet use by healthcare consumers. Indeed, the Internet is often the first destination for a patient recently diagnosed with a health problem.[143] A patient may visit any of a number of healthcare Websites, many of which offer real-time interaction with physicians, health risk assessments, or up-to-date information on a multitude of medical conditions or healthcare questions.[144] However, a patient must often submit a great deal of personal information to receive on-line advice. That information is often left behind or can be traced to its source. When collected and aggregated, this information creates a digital profile that reveals a great deal about an individual's personal life, including her habits of association, speech and commerce.[145]

The Privacy Rule does not address the use of the Internet as a healthcare venue where information is exchanged. Many of the privacy policies espoused by health-care websites fall short of consumers' expectations.[146] Some of these policies do not meet minimum fair-information practices, such as providing adequate notice, giving users control over their information, or holding the sites' business partners to the same privacy standards.[147] Others fail to follow their own stated privacy policies.[148] Nowhere in the Privacy Rule are these shortcomings appropriately addressed.

Medical records, which were already too accessible in paper form, are now even less secure when stored and transmitted on the Internet. The drafting of the Privacy Rule was an opportunity to create more stringent on-line security provisions, but that opportunity was squandered, leaving medical records exposed to potentially unauthorized use by anyone who can access the system.[149] The shortcomings of the

---

[141]Cunningham, *supra* note 56, at 232.

[142]*Id.*

[143]Jeff Goldsmith, *Health Tracking: From the Field; How Will the Internet Change Our Health System?; Powerful though the Internet may be, its impact on health care will continue to be tempered by privacy concerns and professional resistance*, HEALTH AFFAIRS, Jan./Feb. 2000.

[144]A patient might visit www.webmd.com, www.americasdoctor.com, or www.drkoop.com. *See*, Stephen M. Fitzgibbons and Richard Lee, *The Health.net Industry: The Convergence of Healthcare and the Internet*, Hambrecht & Quist, January 1999 *available at* http://medicigroup.com/resources/Resources-HealthNet%20survey.pdf (last visited Feb. 18, 2003, on file with author).

[145]Berman, *supra* note 38.

[146]Janlori Goldman and Zoe Hudson, *Virtually Exposed: Privacy and E-Health; Privacy concerns are keeping consumers from reaping the full benefit of online health information*, HEALTH AFFAIRS, Nov./Dec. 2000. Some of the privacy policies may have changed given the volatility of the Internet.

[147]*Id.*

[148]*Id.*

[149]Goldsmith, *supra* note 143.

Rule and its failure to address changes in the storage and transmission of medical records render it "behind the times," grossly inadequate and obsolete.[150]

2. Exceptions Swallow Additional Privacy Protections

The efficacy of the Privacy Rule is severely diminished because of the numerous instances when patient consent is not required for a disclosure of PHI. For example, non-consensual disclosures of PHI explicitly contemplated in the Privacy Rule include but are not limited to, disclosure:

- to an employer regarding an evaluation of the workplace, a work related illness, or workplace medical surveillance;[151]
- to the FDA to conduct post marketing surveillance, track products, or report biological product deviations;[152]
- to telemarket or mail 'health related products or services' and 'other products of nominal value;'[153]
- to authorized patients pursuant to a court order, subpoena or other court order;[154]
- to a person who may have been exposed to a communicable disease or is at risk of spreading the disease;[155]
- to authorities about victims of abuse, neglect or domestic violence;[156]
- to report child abuse or neglect;[157]
- to oversee healthcare systems, government benefit programs, entities subject to government regulatory programs, or entities subject to civil rights laws;[158]
- under a waiver from an Institutional Review Board or a privacy board according to a series of considerations;[159] or
- to prevent or control disease.[160]

While many of these disclosures might appear legitimate, their scope is so broad that they abrogate a substantial portion of the privacy rights the Rule was intended to create. It is too easy to use any of these reasons as a pretense to disclose PHI without patient consent.

---

[150]Cunningham, *supra* note 56.

[151]45 C.F.R. § 164.512(v).

[152]45 C.F.R. § 164.512(b)(iii).

[153]45 C.F.R. § 164.514(e)(2).

[154]45 C.F.R. § 164.512(f)(1)(ii)(A).

[155]45 C.F.R. § 164.512(b)(1)(iv).

[156]45 C.F.R. § 164.512(c)(i).

[157]45 C.F.R. § 164.512(b)(1)(ii).

[158]45 C.F.R. § 164.512(d)(1).

[159]*See generally*, 45 C.F.R. §164.512.

[160]45 C.F.R. § 164.512(b)(1)(i).

Other non-consensual disclosure situations contemplated by the rule are even less legitimate. For example, allowing the non-consensual disclosure of PHI to telemarket or mail 'health related products or services' and 'other products of nominal value' belies Congressional favoritism for commercial interests.[161] This provision neither bolsters patient privacy nor furthers any articulated public policy. Similarly, allowing the non-consensual disclosure of PHI to law enforcement officials does not infuse a patient with confidence that her personal medical information will remain carefully guarded by her physician. Under-age drinkers, drug users, HIV-positive individuals who have not practiced safe sex, and people who may be a danger to themselves or others might avoid getting needed healthcare for fear that evidence of any crime would be a reason to disclose the information to the police.[162] These scenarios are similar to the *Ferguson* case, and illustrate the "docs to cops" scenario where information given to a physician in confidence is subsequently used in a criminal investigation.[163] They also illustrate how the Privacy Rule chills communication between a doctor and patient as a reasonable patient might not disclose certain information if she feared arrest and criminal prosecution.[164]

Even if a patient does consent to the use or disclosure of PHI, that consent may be neither informed nor consensual.[165] Generally, the consent must: (1) be in plain language, (2) inform the individual that PHI may be used and disclosed to carry out specified activities, (3) indicate that the individual can revoke the consent in writing, and, (4) state that the individual may request that the "covered entity" restrict how PHI is used or disclosed for health care purposes (though the "covered entity" is not required to agree).[166] These provisions are insufficient because a patient might, during the first visit to a physician, sign a consent form that applies to all future disclosures and uses. The patient would not likely know the information she consented to disclose because she typically would not know what is currently in the records.[167] Further, it would be impossible for her to know information that might be contained in future records.[168] Similarly, a patient might be coerced into consenting to disclose PHI as healthcare providers may refuse treatment to a patient who fails to sign an authorization form.[169] Clearly, the "consent" to disclose PHI might be neither informed nor consensual.

The effectiveness of the Privacy Rule is further curtailed because the requirements for patient consent before a disclosure of PHI are not stringent enough. The stated goal of the Privacy Rule was to protect patient privacy by requiring

---

[161]45 C.F.R. § 164.514(e)(2). *See also*, Hatch, *supra* note 29, at 1484.

[162]Swire & Steinfield, *supra* note 3, at 1529-30.

[163]Sobel, *supra* note 42, at 358.

[164]Swire & Steinfield, *supra* note 3 at 1529-30.

[165]Gostin et al., *supra* note 53, at 22.

[166]45 C.F.R. §164.506(c), *cited in id.* at 23.

[167]Gostin et al., *supra* note 53, at 22.

[168]*Id.*

[169]45 C.F.R. §164.506(b)(2), *cited in*, Hatch, *supra* note 29, at 1485.

consent before a disclosure of PHI. Specifying situations in which non-consensual disclosure of PHI is permitted severely reduces the privacy rights that might have been gained. Furthermore, a signed patient consent form must be viewed as suspect because it might not be truly informed, and might have been signed under duress. Either way, these limitations impair a patient's ability to control access to her PHI.[170]

3. The Nebulous Nature of a "Covered Entity"

Many healthcare activities are outside the coverage of the Privacy Rule because they fall into the "gray zone" between traditional healthcare and what the new law covers.[171] By its own terms, the Privacy Rule applies to "covered entities," which consist of healthcare providers, healthcare plans, healthcare clearinghouses, and the business associates of any of these entities.[172] While these terms might seem clear at first blush, ambiguity lurks just below the surface. For example, an entity that appears to be covered might not be if it does not submit claims electronically.[173] Providers who submit paper claims or patients who pay for care out of pocket are therefore not covered.[174] Similarly, the extent to which a "healthcare clearinghouse" is covered is unclear. For example, will all the information collected by a website be covered, or will coverage apply only to information collected for purposes of claims transmission?[175] Much of this ambiguity remains unresolved and will probably only be clarified through court action.

The drafters of the Privacy Rule attempted to mitigate some of this ambiguity by covering an entity's "business associates."[176] A "business associate" assists a "covered entity" in a function involving the use or disclosure of PHI.[177] The "covered entity" is responsible for the conduct of its "business associates,"[178] and if the "covered entity" fails to address a known violation it is deemed to have violated the rule.[179] While this allows HHS to regulate downstream users of PHI,[180] it creates as many problems as it solves by forcing the renegotiation of hundreds of thousands of contracts.[181]

---

[170]Hatch, *supra* note 29, at 1485.

[171]Goldman, *supra* note 146.

[172]45 C.F.R. §160.102, *cited in* Gostin et al., *supra* note 53, at 19.

[173]Goldman, *supra* note 146.

[174]*Id.*

[175]*Id.*

[176]45 C.F.R. §160.103.

[177]Not-for-attribution interview with U.S. Senate Health, Education, Labor and Pensions (HELP) Committee staff member, July 21, 2000, *cited in*, Cunningham, *supra* note 56.

[178]Cunningham, *supra* note 56.

[179]Gostin et al., *supra* note 53, at 20.

[180]*Id.*

[181]Charles N. Kahn, III, president, Health Insurance Association of America, "Confidentiality of Health Information," statement before the Senate HELP Committee, April 26, 2000, *cited in* Cunningham, *supra* note 56.

The ambiguous definition of a "covered entity" and its "business associates" also potentially restricts speech about an individual's PHI.[182] For example, a consumer might be confused over whether an activity is regulated by the Privacy Rule.[183] This would be most common in internet transactions where a consumer might disclose personal health information under the mistaken belief that the website was covered.[184] Conversely, the ambiguity might make a patient reluctant to discuss medical conditions with legitimate members of the healthcare community, including physicians. *Ferguson* addressed this concern, noting that "an intrusion on that expectation [of privacy] may have adverse consequences because it may deter patients from receiving needed medical care."[185]

The failure to adequately define a "covered entity" is not necessarily damning for the Privacy Rule, but it does create unnecessary confusion. The electronic transmission requirement limits entities that are actually covered. Similarly, the extent to which information processed by "healthcare clearinghouses" is covered is unclear. This lack of clarity could have adverse consequences for consumers who might inadvertently disclose personal health information to entities that are not covered. Conversely, consumers might be less willing to speak candidly with legitimate and covered healthcare providers for fear that they are not covered.

4. Federalism Concerns

The Privacy Rule has unresolved federalism conflicts because it seeks to nationalize individual privacy rights, which have traditionally been a state concern. The Rule creates a nationally uniform "floor" of privacy protections by providing that the federal regulation will not preempt state laws that are more stringent in protecting patient privacy.[186] The common law physician-patient privilege illustrates however, that the protection of individual medical privacy has traditionally been a state concern.[187] The intersection of these interests clearly has federalism implications because state and federal interests collide.[188]

Resolving the federalism issue will involve balancing the Supremacy Clause[189] against the 10th Amendment,[190] and the Supremacy Clause will likely prevail. Some academics have argued that the regulation of health information privacy should remain within the ambit of traditional state power.[191] This proposal is problematic however, because it creates multiple standards. For instance, individuals in some

---

[182]Krulwich, *supra* note 91, at 301.

[183]Goldman, *supra* note 146.

[184]*Id*.

[185]*Ferguson*, 532 U.S. at 78, *quoting* Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

[186]45 C.F.R. § 160.203(b). *See also*, Goldman, *supra* note 146, at 398.

[187]Hodge, *supra* note 11, at 793.

[188]*Id*. at 795.

[189]U.S. CONST. art. VI, § 2.

[190]U.S. CONST. amend. X.

[191]Hodge, *supra* note 11, at 807.

states will enjoy greater privacy protections than in others. Similarly, "covered entities" will be required to adhere to both national and State privacy standards.[192] Tipping the balance in favor of adopting a uniform federal regulation are changes in the healthcare industry that make medical records transmission a subject of interstate commerce. As the District Court noted in *The Association of American Physicians and Surgeons*, the Privacy Rule regulates interstate economic activity because healthcare plans operate across state lines.[193] Accordingly, Congress will likely be able to invoke its Commerce Clause powers to nationally regulate the transmission of medical records.[194]

The creation of multiple privacy standards also reveals inconsistencies within the Privacy Rule. The goal of HIPAA was the administrative simplification of the healthcare system.[195] The Rule controverts this goal however, by creating multiple privacy standards. Rather than simplifying the provision of healthcare, the two-tiered approach to privacy protection complicates the provision of healthcare because providers and must comply with both national and regional privacy standards.

The benefit of enacting a uniform national privacy standard was further exemplified in *United States ex rel. Mary Jane Stewart v. The Louisiana Clinic* where the U.S. District Court for the Eastern District of Louisiana easily circumvented a state law that was allegedly more stringent than the federal standard.[196] Relators in a *qui tam* action alleged that Defendants defrauded the federal government by presenting false claims for medical service reimbursements. Defendants, in an effort to protect patient privacy, sought a protective order concerning the disclosure of patient billing and medical records.[197] They argued that they were subject to civil liability under a Louisiana law preventing the disclosure of those records, and that this law was not pre-empted by the Privacy Rule because it exceeded the federal standard.[198]

In requiring that the PHI in question be produced in unredacted form, the court found that the Louisiana statute was not more stringent than the federal standard because the Louisiana law did not address "the form, substance, or the need for express legal permission from an individual" as required by the Privacy Rule.[199] Because the Louisiana law did not fit explicitly within the exception carved out by the Privacy Rule, the "stringency" exception did not apply. Defendants were therefore required to produce unredacted PHI containing patient identifiers.[200] In an

---

[192]Gostin et al., *supra* note 53, at 34.

[193]224 F. Supp. 2d 1115, 1126 (S.D. Tex. 2002) *citing* United States v. Lopez, 514 U.S. 549 (1995).

[194]*Id.* at 1126-27.

[195]Cunningham, *supra* note 56.

[196]No. 99-7767 2002 LEXIS 24062 (E.D. LA), at 5.

[197]*Id.* at *2.

[198]*Id.* at *4.

[199]United State ex rel. Mary Jane Stewart, No. 99-7767 2002 LEXIS 24062 (E.D. LA), at *16, *citing*, 45 C.F.R. § 160.202.

[200]*United State ex rel. Mary Jane Stewart* at *20.

effort to protect the confidential nature of this information the court limited recipients to counsel of record, two paralegals and one expert for each party.[201] The limitation was ineffective however, because the court also concluded that the United States could use information gained in this discovery proceeding in connection with its oversight of healthcare activities.

The impact of this case is threefold. First, it illustrates the benefit of a nationally uniform privacy standard because the addition of the state law caused unnecessary confusion. Absent the state law- federal law controversy, the controlling authority would be clear and the case likely would not have been litigated. Second, the case illustrates how easily the "stringency" provision of the Privacy Rule can be circumvented. Accordingly, this provision creates an ineffective distinction between allegedly more stringent State standards and the national Privacy Rule. Third, the decision illustrates the Rule's shortcoming in protecting individual medical records privacy. While the court sought to limit the disclosure of PHI to counsel of record, two paralegals and one expert for each party, once the PHI is used for government oversight purposes the number of people who could potentially view the unredacted PHI in question is limitless.

5. Congress was Catering to Corporate Interests

A final problem with the Privacy Rule is its suspect motivation. The Rule was passed in an effort to mitigate the consequences of standardizing and streamlining medical records[202] rather than to advance individual privacy interests.[203] It exemplifies an attempt to balance community interests against individual rights,[204] illustrating compromises between privacy advocates and industry leaders.[205] While these compromises were made in an effort to placate those concerned about unwarranted access to medical records, it is important to recall that the Rule does not represent beneficent government action to protect the privacy of personal health information.[206] Rather it is an example of Congress putting "big-money corporate interests ahead of the basic privacy interests of the American people."[207] In considering the efficacy of the Privacy Rule, it is therefore illuminating to recall that it was an afterthought on the heels of administrative simplification. This commercial favoritism, exemplified by permitting the non-consensual disclosure of PHI for marketing and fundraising purposes,[208] can be explained by government officials who succumbed to powerful lobbying groups that have a stake in obtaining personal

---

[201] *Id.* at *19.

[202] Krulwich, *supra* note 91, at 283.

[203] Hatch, *supra* note 29, at 1493.

[204] *Id.*

[205] HHS News, *HHS Proposes Changes That Protect Privacy, Access to Care: Revisions Would Ensure Federal Privacy Protections While Removing Obstacles to Care* (March 21, 2002), *available at* www.hhs.gov/news/press/2002pres/20020321a.html (last visited Feb. 18, 2003, on file with author), *cited in* Davis, *supra* note 18, at 554.

[206] Krulwich, *supra* note 91, at 282-83.

[207] Gostin et al., *supra* note 53, at n. 47.

[208] Hatch, *supra* note 29, at 1493.

health information.[209] While this situation is typical, it is nevertheless important to recall that the government had a pre-textual profiteering motive and was not acting simply to protect individual privacy rights.

VII. ALL IS NOT LOST

> "Change is not made without inconvenience, even from worse to better."[210] -Richard Hooker

The Privacy Rule fails to address significant issues regarding the erosion of medical records privacy. These gaps result from the confluence of increased technology use in medical records storage, the enactment of the Privacy Rule, and the restriction of privacy rights following 9/11, as evidenced by the passage of the USA PATRIOT Act. While the Privacy Rule was ostensibly promulgated in order to protect medical records privacy, its provisions do not go far enough. First, the Rule is based on an out-of-date technology model. Second, the exceptions to the patient consent provisions swallow much of the privacy protection that would have been gained. Third, the Rule fails to adequately define a "covered entity." Fourth, it has unresolved federalist issues. Finally, the supposed privacy protections are suspect because Congress was catering to corporate interests rather than protecting individual rights. Despite these obstacles to creating effective medical records privacy, the government can still protect privacy rights while advancing national security interests.[211]

One of the clearest solutions to problems in the current draft of the Privacy Rule is to change the offending provisions. For instance, the narrow definition of a "covered entity," which allows some entities that deal with PHI to fall outside its coverage, could be broadened to include any entity that deals with PHI. This change would truly protect personal health information by requiring any entity that deals with it to follow the strictures of the Privacy Rule. A broader definition would facilitate enforcement of the Rule by clarifying the guidelines. It would also reduce patient confusion because patients could be secure in their knowledge that any entity to which they submitted PHI would be subject to the Privacy Rule.

Similarly, the conditions under which PHI may be disclosed without patient consent should be narrowed to include only those instances where non-consensual disclosure is absolutely necessary. While there are clearly instances when non-consensual disclosure of PHI is required, those instances must be strictly limited if the Privacy Rule is to have any substantial effect.

The decision to disclose PHI without patient consent should be considered against the backdrop of the physician-patient privilege. This tradition protects conversations between physician and patient and clearly exists because of the intimate nature of personal health information. The legislature should defer to tradition in this instance, treading carefully before abrogating this important and fundamental duty of confidentiality. Similarly, legislators should be particularly

---

[209] *Id.*

[210] Samuel Johnson, DICTIONARY OF THE ENGLISH LANGUAGE, (1755) *available at* http://www.bartleby.com/66/28/28828.htm (last visited Feb. 17, 2003, on file with author).

[211] Swire & Steinfield, *supra* note 3, at 1539.

careful to protect the privacy of personal health information in light of the threat to medical records privacy posed by the increased use of technology. They should recognize the relevance of a long-standing protection, and utilize it to account for continuing changes in the use of technology.

Technology however, can be used to increase medical records security. In passing HIPAA, Congress recognized the shift to electronic storage and transmission of medical records. In addition to allowing for the standardizing and streamlining of medical records, this shift also provides an opportunity to implement sound data handling practices throughout the healthcare industry.[212] Technology companies currently have available privacy enhancing features such as encryption, on-line opt-in buttons, and anonomymizers that can be used to increase security on the web, in e-mail transmissions, and in data storage.[213] These devices should be used to increase the security of personal health information, which will facilitate greater medical records privacy by carefully controlling who has access to information storage and transmission systems and how such access is regulated.

Because the judiciary will ultimately interpret enforcement of the Privacy Rule, it should be drafted to consistently protect medical records privacy. This may be accomplished by upholding a patient's "reasonable expectation of privacy."[214] The current draft of the Rule moved in that direction by establishing a "floor" of privacy protections, but the solidity of this "floor" is questionable because it has unresolved federalism issues. Congress might therefore be justified in pre-empting State legislation on medical records privacy issues under the Commerce Clause, which would eliminate discrepant standards between States, facilitate compliance by "covered entities," and provide patients with a uniform standard of protection.

In changing the text of the Privacy Rule, HHS might also consider internal restructuring in order to more effectively deal with privacy issues. For instance, HHS could create a system similar to the issuing of a temporary restraining order where a "covered entity" must contact a judge or regulatory agency before disclosing PHI without patient consent. That judge or agency could be empowered to quickly decide whether the non-consensual disclosure of PHI is warranted. Similarly, HHS could appoint regional staff members who would be consulted about non-consensual disclosures of PHI. HHS could also create a sub-agency to deal specifically with medical records privacy issues. These new agencies or staff members might operate as a board, or as a quasi-judicial system that would decide whether non-consensual disclosures of PHI are warranted. Whatever form this institution would take, its goal should be to ensure that a patient's reasonable expectation of privacy remains relatively constant.

VIII. CONCLUSION

"Law is order, and good law is good order."[215] -Aristotle

---

[212] *Id.* at 1518.

[213] Goldman, *supra* note 147.

[214] *Ferguson v. City of Charleston*, 532 U.S. 76, 78 (2001).

[215] POLITICS, bk. VII, ch. 4, *quoted in*, JOHN BARTLETT, FAMILIAR QUOTATIONS 98 (Little, Brown and Co.1968) (1855).

The protection of medical records privacy is an important and pervasive issue. While individual privacy rights had expanded prior to 9/11, they have been severely restricted following those tragic events. In light of contracting privacy rights, the protection of medical records privacy becomes even more important, particularly when one considers that privacy is more easily subject to transgression as a result of the increased use of technology to store and transmit medical records, and the enactment of the USA PATRIOT Act. Accordingly, the Privacy Rule, which was promulgated in an effort to protect individual medical privacy rights, must be re-examined to ascertain whether it can withstand these new challenges.

Upon re-examination of the Privacy Rule, its shortcomings become glaringly apparent. While this does not mean that the Privacy Rule must be discarded, it indicates that the Rule must be altered if substantial privacy protection is to be preserved. These alterations include broadening the scope of the Rule and requiring that currently available technology security devices be utilized to substantially protect the privacy of medical records. Congress should also consider pre-empting State privacy protections in favor of a uniform national standard, as well as restructuring agencies in order to provide meaningful privacy protection. Through this continued re-tooling of the Privacy Rule, Congress can defend against the tripartite threat to medical records privacy, and in so doing preserve individual privacy, dignity and autonomy.

NATHAN J. WILLS[216]

[216]J.D. 2004, Cleveland-Marshall College of Law, B.A. 2000, Denison University. The author would like to thank his family an friends for their support, and Professor Karin Mika for her help.