Vanderbilt Law Review

Volume 53
Issue 5 *Issue 5 - October 2000*

Article 15

10-2000

Protecting Health Information Privacy: the Case for Self-Regulation of Electronically Held Medical Records

Catherine L. Glenn

NOTES

Protecting Health Information Privacy: The Case For Self-Regulation of Electronically Held Medical Records

I. INTRODUCTION

Advances in technology have given new life to debates concerning privacy.[1] Specifically, issues surrounding increased access to personal medical records have recently garnered attention. On one side of the debate, healthcare providers and insurers support

1. *See, e.g.*, Sandra Byrd Petersen, *Your Life as An Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163 (1995).

expanded access to medical records for treatment, research, and insurance claims purposes. At the same time, however, many patients legitimately expect their medical records to remain private. The advent of Internet access to patient records and electronic medical insurance claims submissions has heightened patients' concerns that computerized medical records will offer less protection and more potential for unauthorized disclosure than paper files in locked cabinets.[2] This has prompted commentators to argue that, as medical information becomes increasingly accessible via means outside a patient's control, the need for privacy protection grows even stronger.[3] Though threats to privacy exist in all media of information, electronically stored information lies particularly vulnerable to abuse and thus requires heightened protection.[4]

For example, one former employee of a state health plan discovered during a computer training class that he could access records of several insurance subscribers.[5] When he typed in his own name, he was startled to see his private psychiatric records, including the name of the antidepressant medication he was taking.[6] Similarly, one woman who had purchased a used computer found 2,000 patient records from a pharmacy that had simply been left stored on the computer's hard drive.[7] These records contained the names, addresses, Social Security numbers, and lists of every medication prescribed for customers of the pharmacy, including prescriptions for AIDS and psychiatric conditions.[8] A third illustration shows the unique dangers of electronic websites: one chief executive officer of a loan company that allows customers to apply for credit cards and loans on-line initiated a strict privacy policy.[9] Though he took several steps to safeguard customer privacy—including bar-

---

2. *See* Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, 25 WM. MITCHELL L. REV. 223, 226-27 (1999).

3. *See* CHARLES J. SYKES, THE END OF PRIVACY 100-03 (1999); Roger E. Harris, *The Need to Know Versus the Right to Know: Privacy of Patient Medical Data in an Information-Based Society*, 30 SUFFOLK U. L. REV. 1183, 1196 (1997) (footnote omitted).

4. *See id.* One commentator stated the problem in stark terms: "New technology dramatically expands the potential for abuse. 'Data is like a prostitute,' says one advocate for the mentally ill. 'Once it's on the street, everybody has access to it.' " SYKES, *supra* note 3, at 101.

5. *See* SYKES, *supra* note 3, at 101.

6. *See id.* After this experience, the trainee stated, "I can tell you unequivocally that patient confidentiality is not eroding—it can't erode, because it's simply nonexistent." *Id.*

7. *See id.*

8. *See id.* Upon further investigation, the woman learned that as many as thirty-four other computers had been sold carrying similar medical information. *See id.*

9. *See* Michael Moss, *A Web CEO's Elusive Goal: Privacy*, WALL ST. J., Feb. 7, 2000, at B1.

ring his technicians from using "cookies,"[10]—the CEO was stunned to learn that parts of his Web site did in fact employ cookies.[11] The cookies were placed on the site as a result of the company's acquisitions and mergers with other Internet lenders who allowed the use of cookies on their websites, even though the company had paid $250,000 for a privacy audit conducted by an outside firm.[12]

The effects of the increasingly unauthorized disclosure of private medical information are evident in both individual behavior and in the quality of health care that patients receive. For example, a recent poll found that one in six United States adults "had at some time done something unusual to conceal medical information, such as paying cash for services."[13] One commentator noted that some patients may even stop treatment when they begin to suspect that their privacy is not being respected.[14] In addition, numerous psychologists admit to avoiding discussions of sensitive material that could prove damaging if such information ended up on insurance company databases.[15] In contrast, one Baltimore psychiatrist told the *Washington Post* that economic incentives encourage doctors to probe into deeply sensitive areas because the more specific a record is, the more insurance approvals the therapist will receive.[16] Either way, these examples show how privacy problems create incentives for doctors and patients to engage in behavior that can often thwart the common goal of effective health care.[17]

Given the potential consequences, it is not surprising that people take extraordinary measures to protect the privacy of their

---

10. *Id.* Cookies are computer codes that track visitors to Internet sites. *See id.* Using cookies allows information that a customer has stored on a computer hard-drive or entered at a website to be transmitted to other sites without the customer's awareness. *See id.*

11. *See id.*

12. *See id.* When the CEO asked the other lenders to remove cookies from their shared sites, he learned that this was impossible since the other lenders had pacts with other partners to use cookies. These pacts allowed the partners to receive a bounty every time they referred someone to their sites. *See id.*

13. SYKES, *supra* note 3, at 101. Paying cash for services ensures that there is no way the services will be traceable through financial means, such as credit card or bank statements.

14. *See id.* at 105 ("Many [doctors] can recount stories of patients who have dropped out of treatment when they were told their confidences might not be respected. Other patients have walked out when told that their therapist would have to label them with a mental disorder to justify continued coverage with the insurance company.").

15. *See id.* at 105 ("Some therapists confess that they have found themselves almost unconsciously steering away from information in their sessions that might prove to be damaging if it made its way into the computerized databases of insurance companies.").

16. *See id.* (citing Arthur Allen, *Exposed: Computer Technology, Managed Care Are All Undermining the American Tradition of Medical Privacy, In the Name of Progress*, WASH. POST, Feb. 8, 1998).

17. *See supra* notes 14-15.

medical records. Indeed, unauthorized disclosure can result in a patient being denied insurance, deciding to forego insurance, getting fired, or being stigmatized.[18] In one instance, an employer discovered that an employee had AIDS from a pharmacy's computer printout that mistakenly included patient names.[19]

The potential for unwarranted release of personal medical information due to the increased popularity of electronic storage databases has spawned a debate over the types of remedies that will best protect individual privacy.[20] There are several potential tools for balancing a patient's privacy concerns with the interests of other parties in accessing medical information.[21] These include state law, federal law, self-regulation,[22] and explicit federal constitutional protection.[23]

---

18. Privacy experts have articulated three types of harms that can result from privacy violations within the realm of medical information. *See* Harris, *supra* note 3, at 1196-97 (footnote omitted). First are "intrinsically moral violations" that violate an individual's interest in protecting personal information from disclosure. *See id.* Second are consequential harms, which have effects beyond the individual level and "elicit responses from society as a whole." *Id.* These releases often result in social stigmas that attach te a person as a result of disclosures of information regarding sensitive social issues such as HIV/AIDS or psychiatric counseling. *See id.* The third type of harm is financial. *See id.* An example of a financial harm would be a scenario where an employee loses her job or a cancer-patient is denied a loan because of a non-consensual release of private medical information. *See id.*

19. *See* Doe v. Southeastern Pa. Transp. Auth. ("SEPTA"), 72 F.3d 1133, 1135 (3d Cir. 1995). The Southeastern Pennsylvania Transportation Authority ("SEPTA") did not fire Doe as a result of his illness; rather, Doe brought his claim under 42 U.S.C. § 1983, alleging that the company violated his right to privacy. *See id.* at 1134-35; *see also infra* notes 83-91 and accompanying text.

20. *See, e.g.*, Harris, *supra* note 3, at 1191. Medical records are particularly difficult te regulate because they have various uses. This variety means that lawmakers attempt to write healthcare laws to protect groups with different interests, such as patients and insurance providers. The resulting law is often an attempt to strike a middle ground that pleases neither group. Additional uses can include patient care, communication between doctors, documenting care for insurance purposes, research, complying with a legal duty, obtaining payment and defending a health care provider in a malpractice suit. *See id.*

21. State intrusion inte personal information creates different problems and must be regulated differently than intrusion by private third parties. This distinction is discussed more extensively below. *See infra* Part III.B.

22. Self-regulation is a term that is used in a variety of ways. In the context of this Note, it refers to regulation that exists because of the initiative of the entity that would otherwise be regulated by the government at some level. For a general discussion and list of reference materials discussing the various uses of and debates concerning the term "self-regulation," see Matthew J. McCloskey, *Bibliography of Internet Self Regulation, Internet Law and Policy Forum* (visited Feb. 23, 2000) <http://ilpf.org/selfreg/bib4_15.htm>. There are a wide range of self-regulatory tools, including codes of conduct, voluntary standards, accreditation, third-party certification and audits. *See id.* at <http://ilpf.org/selfreg/announce.htm>.

23. *See, e.g.*, Carter, *supra* note 2, at 241; *see also* Robert Gellman, *Does Privacy Law Work?, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 195 (Philip E. Agre & Marc Rotenberg eds., 1997). Gellman points out that American privacy law is fragmented, while privacy law in Europe is usually governed by omnibus rules that apply generally te both pub-

To help preserve an individual's right to privacy, a number of states have enacted comprehensive schemes to regulate the dissemination of private medical information within their boundaries.[24] Many state constitutions, for example, include constitutional amendments designed to protect private information.[25] In addition, common law remedies remain available for invasions of privacy.[26] Still further, several states have enacted legislative schemes designed to protect a resident's private medical information.[27] Moreover, many of the techniques that states use to create privacy protections mirror those used at the federal level and have similar defects.[28]

In addition to the actions taken by the individual states, the federal government has proposed—but not passed—privacy protection legislation.[29] The 1996 Health Insurance Portability and Accountability Act ("HIPAA") gave Congress until August 21, 1999 to pass legislation pertaining to medical records privacy, but Congress failed to meet this deadline.[30] As a result, the burden of proposing appropriate privacy regulations fell on the Department of Health and Human Services ("HHS") and President Clinton.[31] On October

---

lic and private records. The American approach is "secteral," meaning that instead of implementing laws to protect privacy in general, such laws cover specific records or recordkeepers. The effect of this approach is what is often described as a patchwork quilt of privacy law, spread among constitutional protections, common law remedies and statutory protections.

24. *See* Carter, *supra* note 2, at 246-51 (summarizing the various techniques states use to protect privacy).

25. *See id.* at 246 (citing to the constitutions of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington).

26. *See id.* at 247 (discussing state law claims for hreach of fiduciary duty of confidentiality, invasion of right to privacy, and breach of implied contract).

27. *See id.* at 254-66 (using as examples state legislation in California, Tennessee, and Minnesota).

28. *See generally id.* (surveying the problems inherent with state as well as federal privacy protections).

29. *See, e.g.*, Shailagh Murray, *White House Seeks Compromise on Access to Health Information*, WALL ST. J., Oct. 25, 1999, at A4 ("On Capital Hill, lawmakers' many attempts to forge privacy legislation have sputtered.").

30. *See* Mary Jane Fisher, *Senate Stymied on Medical Privacy Legislation*, NAT'L. UNDERWRITER PROP. & CASUALTY–RISK AND BEN. MGMT. June 21, 1999, *available in* 1999 WL 8859623. There are three main reasons cited for the failure of the bill's passage: First was a party conflict over whether a minor's medical records would trigger notification to parents of pregnancy or AIDS. Second was whether there could be a "right to sue" for violations of medical confidentiality law. Third was whether a federal privacy law should preempt state laws. *See id.*

31. *See* Health Insurance Portability & Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996) (codified in sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C. (also referred to as the Kennedy Kassenbaum Act)). The terms of HIPAA dictated that, should Congress fail te act by its self-imposed deadline, the burden of regulating medical records

29, 1999, President Clinton proposed several regulations scheduled for implementation in February 2002.[32] These regulations would require drug companies and other entities to gain approval from a review board before being allowed access to individually identifiable patient information without patient consent.[33] The regulation allows HHS to restrict the conduct of health plans and providers, but it precludes the department from regulating those who might receive private medical records, such as pharmaceutical companies or other contractors.[34]

In addition to the legislative approach, federal constitutional protection of privacy interests remains a possibility, although prior case law fails to provide an absolute endorsement of individual privacy rights. In the 1977 decision of *Whalen v. Roe*, the United States Supreme Court upheld a New York law requiring doctors to report to the state all prescriptions written for certain dangerous or narcotic drugs.[35] The Court held that this requirement did not unconstitutionally invade the patients' privacy interests, and the majority decision declined to explicitly establish a constitutional right to privacy in one's medical records.[36]

In light of the fact that technological advances are making private medical information more easily available, the Court's reluctance to articulate a clear privacy standard troubled Justice Brennan, who noted in his concurring opinion that

> [t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[37]

---

privacy would fall to the Department of Health and Human Services and President Clinton. *See id.*

32. *See* Lisa M. Bowman, *Clinton Privacy Plan: Only a First Step*, ZD New News from ZD Wire, (Oct. 29, 1999), *available in* 1999 WL 14538191.

33. *See HHS Privacy Reg Seeks to Protect Subjects in Privately-Funded Studies*, HEALTH NEWS DAILY, Nov. 1, 1999, *available in* 1999 WL 10485071.

34. *See id.*

35. Whalen v. Roe, 429 U.S. 589, 605 (1977) (holding that the New York law evidenced a proper concern for the privacy interests of the individuals involved).

36. *See id.* Although there is no "general constitutional right to privacy," the Supreme Court has found privacy protection to emanate from the Constitution in specific instances. *See, e.g.*, Katz v. U.S., 389 U.S. 347, 350 (1967) (finding that a right to privacy emanates from the Fourth Amendment); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (finding that a right to privacy emanates from the penumbra of the First Amendment).

37. *Whalen*, 429 U.S. at 607. For example, early in 1999, a major medical center inadvertently stored several thousand patient records on a public Internet site for two months. *See President Clinton Takes New Steps to Protect the Privacy of Personal Health Information*, M2 Presswire, Nov. 1, 1999, *available in* 1999 WL 24365493. Similarly, during a speech to unveil

Since 1977, technology has indeed increased the accessibility of medical records via electronic media. Meanwhile, technology also has diminished the effectiveness of existing methods, such as locked cabinets, file rooms and security personnel, of protecting secret information from falling into the wrong hands.[38]

Without clear guidance from the Supreme Court, the circuits have split on the issue of whether the Constitution protects the privacy of one's medical records from unauthorized intrusion. The Sixth Circuit has found that no such right exists,[39] and the Third Circuit has vehemently disagreed.[40] In light of the Court's past decisions pertaining to the constitutional right of privacy, the Court should revisit this issue because of the drastic changes in access to medical information since the *Whalen v. Roe* decision.[41]

Along with legislation and constitutional protection, self-regulation is a potential solution that has received increasing attention due to the increased popularity of the Internet. Although any self-regulatory model would require outside regulatory measures and incentives to succeed, such a model may provide the best

---

his proposed privacy-protection plan, President Clinton noted a survey "showing that one-third of all Fortune 500 companies check medical records before they hire or promote people." Bowman, *supra* note 32. Another example concerns a mother who submitted bone marrow cells te a bank in order te be screened to determine whether she matehed the marrow of her young daughter who was suffering from a bone marrow disease. There was no match, and the girl died, but the woman's results from the screening ended up in a computerized database, subjecting the mother to hundreds of phone requests for her bone marrow. *See* Leah Curtin & Roy Simpson, *Privacy in the Information Age?*, HEALTHY MGMT. TECH. 32, Aug. 1, 1999, *available in* 1999 WL 13225148. Other instances include a Florida healthcare worker who leaked a confidential list of AIDS patients to newspapers, a medical student who sold medical records to malpractice lawyers, Medicaid clerks who sold computer printouts of patient financial records te managed care companies, and a convicted rapist who stole someone else's password to browse over 1000 patient files in order to obtain telephone numbers and privato information before making obscene telephone calls. *See id.*

38. In September 1999, computer backers circulated a phone number that allowed anyone to access a database of private medical records stored at St. Joseph Mercy Hospital in Pontiac, Michigan. The hospital bad been using a digital system that let doctors dictate medical records. *See* Bowman, *supra* note 32.

39. *See* Jarvis v. Wellman, 52 F.3d 125, 126 (6th Cir. 1995) ("Disclosure of plaintiff's medical records does not rise to the level of a breach of a right recognized as 'fundamental' under the Constitution.").

40. *See* Doe v. SEPTA, 72 F.3d 1133, 1138 (3d Cir. 1995) (holding that employee medical records deserve a measure of constitutional protection); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-78 (3d Cir. 1980). Although the Third Circuit found such a constitutional protection to exist, it refused to find that the plaintiff's constitutional right was violated, thus weakening the practical impact and arguably the precedential value of such a right. *See Westinghouse*, 638 F.2d at 576.

41. *See* Petersen, *supra* note 1, at 172. ("Despite Justice Brennan's explicit recognition tbat changing technology may necessitate a reexamination of this issue by the Court, this issue has not resurfaced for reconsideration.").

method of protecting electronically stored health information and medical records.[42]

This Note argues that a comprehensive model of self-regulation, supplemented by market incentives and the threat of strong federal legislation to supplant failed self-regulation, constitutes the most practical and effective means of protecting medical records stored in electronic formats. Part II of this Note examines the historical and legal background of the medical records privacy issue, focusing on the difficulties encountered by courts attempting to resolve the issue under the Constitution. Part III then surveys current state legislation and the pending federal and administrative solutions and offers an argument for why these solutions are by themselves insufficient. Part IV examines the debate over self-regulation of Internet privacy and considers examples of successful self-regulation in other industries. This Note concludes by advocating more comprehensive attempts at self-regulation of electronically stored medical records, along with continued congressional attempts to pass satisfactory federal legislation to supplement self-regulation.

II. HISTORICAL PRECEDENT AND THE CURRENT STATUS OF CONSTITUTIONAL PRIVACY PROTECTION FOR PATIENT MEDICAL RECORDS

Existing privacy protections are ill-equipped to confront the privacy problems created by technology. Older models such as the Hippocratic Oath[43] leave discretion entirely in the hands of the physician, while constitutional protections lack the capacity to protect privacy invasions from private actors seeking personal information.

A. The Hippocratic Oath

The earliest assertions of the need to protect private medical information gave physicians the exclusive power to protect patient privacy. For example, the Hippocratic Oath reads as follows:

---

42. *See infra* Part IV.

43. The Hippocratic Oath is "an oath embodying a code of medical ethics taken by those about to begin medical practice." WEBSTER'S NEW COLLEGIATE DICTIONARY 542 (1974). According to one author, "[h]is oath suggests that privacy of a patient's medical information creates the foundation upon which a patient reposes trust in his or her physician." Harris, *supra* note 3, at 1183.

> [w]hatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning all that should be kept secret.[44]

This rule, while still extant within the medical profession, becomes less applicable in the current context of the technologically advanced health care industry and its rules and regulations, because total responsibility for a patient's well-being rarely rests in the hands of a single doctor.[45]

B. The History of a Constitutional Right to Privacy and Whalen v. Roe

In 1890, Samuel Warren and Louis Brandeis introduced the concept of an individual right to privacy.[46] Beyond a mere property right, the right to privacy protects the underlying intellectual expectation of privacy that arises from the secure ability to prevent public disclosure of personal information.[47] Foreshadowing many of the current issues accompanying the increased availability of electronically stored personal medical information, Warren and Brandeis noted that technological advances like cameras and high speed newspaper printing presses had "invaded the precincts of private and domestic life."[48] In this sense, Warren and Brandeis viewed privacy as a means to preserve personal dignity.[49]

Almost seventy years later, in *Griswold v. Connecticut*,[50] the Supreme Court for the first time implied a constitutional right of

---

44. TABER'S CYCLOPEDIA MEDICAL DICTIONARY 769 (15th ed. 1985) (quoting the Hippocratic Oath).

45. *See* SYKES, *supra* note 3, at 102 (quoting a managed care executive as saying that "Hippocrates is 2,000 years old .... Medicine isn't one-on-one anymore. It's a team effort."). Sykes notes that those who might have access to medical information include "HMO's, insurance companies, private and public databases, pharmacists, hospital workers, and employers." *Id.* In the managed care situation, that list might be expanded to include state health organizations, researchers and marketing firms. *See id.*

46. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197-99 & n.1 (1890) (arguing that a general right to privacy affords a remedy for mental pain).

47. *See id.* at 201-205 ("[T]he protection afforded to thoughts, sentiments, and emotions . . . is merely an instance of the enforcement of the more general right to be let alone.").

48. *Id.* at 195.

49. *See id.*

50. *Griswold v. Connecticut*, 381 U.S. 479 (1965). In *Griswold*, the Director of Planned Parenthood of Connecticut and a Connecticut physician were convicted of violating a Connecticut law prohibiting the use or dissemination of any birth control device. *Id.* at 480. The Supreme Court held that the law unconstitutionally intruded on the right of marital privacy found in the "zone of privacy created by several fundamental constitutional guarantees." *Id.* at 485.

privacy independent of the Fourth Amendment.[51] *Griswold* signaled an analytical shift from the rights-based approach utilized in prior Fourth Amendment cases toward a broader interpretation of constitutional interests.[52] The Court balanced a patient's personal interests in protecting against unwarranted intrusion into private areas with the government's interest in accessing such areas.[53] Commentators have argued that as a result of this shift in reasoning, "the clear trend has been the expansion of privacy rights."[54] Though the Court in *Griswold* issued four separate opinions in defense of its judgment, the reasoning of each of the opinions demonstrated the existence of a privacy right distinct from the Fourth Amendment.[55] Subsequent decisions such as *Loving v. Virginia*,[56] *Stanley v. Georgia*,[57] and *Eisenstadt v. Baird*,[58] upheld and reinforced the privacy rights of individuals. Each of these cases recognized a legitimate constitutional privacy right by weighing that right against the gov-

---

51. *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS AND THE RISE OF TECHNOLOGY 22 (1997) (noting that *Griswold* began the "trend [toward] the expansion of privacy rights").

52. The Fourth Amendment is a likely place to find constitutional protection of private medical records. *See* John Godfrey, *Forbes Hits "Assault" on Medical Privacy*, WASH. TIMES, Dec. 17, 1999, at A8. ("[T]he Constitution's prohibitions against unreasonable searches and seizures are adequate to protect against invasions of personal privacy by law enforcement."). The Supreme Court, however, has found other constitutional protections independent of the Fourth Amendment. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 166 (1973) (finding that a state law prohibiting abortion under any circumstance except to save the life of the mother was an unlawful invasion of an individual's constitutional, non-Fourth Amendment privacy rights); Eisenstadt v. Baird, 405 U.S 438, 453 (1972) (using penumbral privacy rights to invalidate a stato law prohibiting the distribution of contraceptives to unmarried individuals); *Griswold*, 381 U.S. at 485 (holding that various constitutional "penumbral rights" exist to provide privacy protection and render a stato law forbidding the use of contraceptives unconstitutional).

53. *See supra* note 51 (discussing the Court's shift toward "a utilitarian cost-benefit analysis which balances the costs to privacy and the benefits to public safety").

54. *Id.* DeCow argues that the reasoning in *Griswold* was anticipated by similar constitutional arguments protecting privacy in the case of *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905). *See id.* at 23.

55. *Griswold*, 381 U.S. at 485 ("We have had many controversies over these penumbral rights of 'privacy and repose.' [Past Supreme Court cases] bear witness that the right of privacy which presses for recognition here is a legitimate one. The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees.") (citing Lanza v. New York, 370 U.S 139l (1962); Monroe v. Pape, 365 U.S. 167 (1961); Frank v. Maryland, 359 U.S. 360 (1959); Skinner v. Oklahoma, 316 U.S. 535 (1959); Public Utils. Comm'n v. Pollack, 343 U.S. 451 (1952); Breard v. City of Alexandria, 341 U.S. 622, 626, 644 (1951)).

56. Loving v. Virginia, 388 U.S. 1, 2 (1967) (striking down a Virginia statute outlawing intorracial marriage based on the Court's recognition of a penumbral privacy right).

57. Stanley v. Goorgia, 394 U.S. 557, 559 (1969) (citing a penumbral privacy right as an important justification for allowing obscene materials in one's home).

58. Eisenstadt v. Baird, 405 U.S. 438, 443 (1972) (citing a penumbral privacy right as the rationale for allowing distribution of contraceptive devices).

ernmental interests in limiting or intruding upon it.[59] Finally, in *Roe v. Wade*, the Court concluded that there are circumstances where an individual's right to privacy outweighs the state's interest in protecting a potential life.[60] *Roe* served as a strong statement in support of a fundamental right to privacy and its relative weight when compared to competing governmental interests.

Using *Roe* as a foundation, the Court in *Whalen v. Roe* issued its most comprehensive definition of the privacy right, acknowledging both an "individual interest in avoiding disclosure of personal matters" and an "interest in independence in making certain kinds of important decisions."[61] *Whalen* is particularly relevant to the issue of medical records privacy, because it involved the constitutionality of a New York law mandating centralized computer record keeping of prescriptions for certain drugs, complete with patient-identifiable information.[62] Although the Court upheld the statute at issue,[63] the reasoning employed by the Court is encouraging for three reasons. First, the Court recognized a more comprehensive privacy right, including an "interest in avoiding disclosure of personal matters" that could encompass one's right to resist law enforcement intrusion into personal medical information.[64] Second, the Court's balancing test focused on the potential harms caused by the collection and maintenance of such information in medical databases; only after the Court was satisfied that the privacy risks were sufficiently protected did it acknowledge the state's interest in collecting such data.[65] Finally, Justice Brennan's concurrence rec-

---

59. *See id.* at 453; *see also Stanley*, 394 U.S. at 567; *Loving*, 388 U.S. at 12.

60. Roe v. Wade, 410 U.S. 113, 150, 162-63 (1973) (acknowledging a state interest in protecting potential life, but concluding that this interest does not completely outweigh the privacy right of the mother). The Court, however, has issued opinions on related issues that resolve this balancing in favor of the governmental intrusion. *See, e.g.*, Planned Parenthood v. Casey, 505 U.S. 833, 887 (1992) (finding that Pennsylvania's informed consent restrictions on abortion rights did not impose an undue burden on the individual's constitutional privacy rights); Webster v. Roproductive Health Servs., 492 U.S. 490, 507 (1989) (finding that a state's interest in promulgating a law banning public employees from performing nontherapeutic abortions in public facilities outweighed the individual's constitutional interest); Bowers v. Hardwick, 478 U.S. 186, 196 (1986) (upholding a Georgia statute criminalizing sodomy).

61. Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

62. *Id.* at 591 (addressing "whether the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and unlawful market").

63. *See id.* at 603-04 (finding that the potential privacy threats inherent in New York's Controlled Substances Act did not rise to an unconstitutional "invasion of any [privacy] right or liberty").

64. *Id.* at 599.

65. *See id.* at 593-94 (finding that protections such as locking the data tape in a storage facility when not in use, running the data off-line, and providing access to only a limited num-

ognized that state access to personal records was troublesome, and that future technological developments might create a need to revisit the balancing process and to restrict the government's use of technology that places privacy rights at risk.[66]

Despite the *Whalen* Court's cautionary language,[67] lower courts have read the decision as severely limiting the right to informational privacy, thereby shifting the balance toward governmental interests.[68] *Whalen* set the Court's deferential tone in considering the weight appropriately accorded to governmental activities when it observed that numerous state actions "require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."[69] According to one commentator, subsequent circuit court cases indicate that deference to government interests has be-

---

ber of officials were sufficient to ensure confidentiality); *see also id.* at 598 ("At the very least, it would seem clear that the State's vital interest in controlling the distribution of dangerous drugs would support a decision to experiment with new techniques for control.").

66. Justice Brennan observed:

> What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows, the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

Id. at 606-07 (Brennan, J., concurring).

67. The *Whalen* Court noted that:

> The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosure. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence of a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.

See id. at 605-06

68. *See* Doe v. SEPTA, 72 F.3d 1133, 1139-40 (3d Cir. 1995) (finding that an employer's need to access prescription records outweighed the employee's privacy interest in a case in which an employer discovered that an employee had AIDS based on the employee's drug purchases via an employee health plan); United States v. Westinghouse, 638 F.2d 570, 580 (3d Cir. 1980) (finding that the strong public interest in facilitating research and investigations of the National Institute for Occupational Safety and Health justified the intrusion into privacy surrounding employee medical records).

69. *Whalen*, 429 U.S. at 605.

come almost impossible to overcome.[70] As a result, the Court's interpretation of the Constitution makes it likely that "almost any police action intruding upon private medical records would currently survive such judicial review."[71]

C. Lower Court Precedent

Three years after the *Whalen* decision, the Third Circuit expanded upon its tentative framework in *United States v. Westinghouse*.[72] In *Westinghouse*, an employer appealed a district court decision granting a motion to direct the employer to produce certain documents in accordance with a subpoena *duces tecum* issued by the Director of the National Institute for Occupational Safety and Health ("NIOSH").[73] The employer argued that requiring disclosure of employee medical records would violate the privacy interests of the employees.[74]

The Third Circuit Court of Appeals noted that employee medical records fall "well within the ambit of materials entitled to [constitutional] privacy protection."[75] In order for a court to allow "intrusion into the zone of privacy surrounding medical records, it [must find] that the societal interest in disclosure outweighs the

---

70. *See* Peter H.W. van der Goes, Jr., Comment, *Opportunity Lost: Why and How to Improve the HHS-proposed Legislation Governing Law Enforcement Access to Medieal Records*, 147 U. PA. L. REV. 1009, 1036 (1999) ("[W]hen courts employ a flexible balancing approach and the government can assert some legitimate purpose, many privacy interests appear insufficient te overcome the courts' deference to the State.").

71. *Id.*

72. *Westinghouse*, 638 F.2d at 570.

73. *See id.* at 573. The purpose of the subpoena was to establish whether employees' medical records would support the claim that the plant employees were exposed to a hazardous substance known as hexahydrophtbalic anhydride, or HHPA. *See id.* at 573.

74. *See id.* at 574.

75. *See id.* at 577. The Third Circuit explained:

> Information about one's body and state of health is [a] matter which the individual is ordinarily entitled to retain within the "private enclave where he may lead a private life." It has been recognized in various contexts that medical records and information stand on a different plane than other relevant material. For example, the Federal Rules of Civil Procedure impose a higher burden for discovery of reports of the physical and mental condition of a party or other person than for discovery generally. . . . Medical files are the subject of a specific exemption under the Freedom of Information Act. 5 U.S.C. § 552(b)(6) (1976). This difference in treatment reflects a recognition that information concerning one's body has a special character. The medical information requested in this case is more extensive than the mere fact of prescription drug usage by identified patients considered in *Whalen v. Roe* and may be more revealing of intimate details. Therefore, we hold that it falls within one of the zones of privacy entitled to protection.

Id. at 577.

privacy interest on the specific facts of the case."[76] Thus, to properly balance these competing interests, the *Westinghouse* court developed a seven factor test to be used in deciding whether an intrusion into an individual's privacy is justified.[77]

After applying the test to the facts of the case, the court noted that the interests in occupational safety and employee health in a particular plant ranked as high as other public interests previously found to justify intrusion into information areas normally considered private.[78] The court also emphasized the high need for accessibility to the entire medical file of employees in order to determine whether, and more importantly, when, employees had been subjected to hazardous substances.[79]

Furthermore, the court noted that the employer had not provided any evidence indicating that the information contained in the medical records was particularly sensitive, or that the potential intrusion would be especially severe to the welfare of its employees.[80] Because the company conducted the testing and examination of employee medical records with the purpose of protecting individual employees from potential hazards, the court held that such measures would not likely deter employees from undergoing periodic medical examinations.[81]

Finally, the court considered the adequacy of the safeguards implemented to protect the compiled medical information.[82] Based on the district court's observation that company procedures for protecting the records and removing names and addresses of the individuals in the compilation of data constituted sufficiently adequate protection against non-disclosure, the Third Circuit agreed that the employee's information had adequate protection.[83] The court did not

---

76. *Id.* at 578.

77. *Id.* The seven factors are: the type of record requested; the information it does or might contain; the potential for harm in any subsequent nonconsensual disclosure; the injury from disclosure to the relationship in which the record was generated; the adequacy of safeguards to prevent unauthorized disclosure; the degree of need for access, and whether there is an express statutory mandate; and articulated public policy or other recognizable public interest militating toward access. *See id.* The court did not indicate whether all of the factors must be met before access to private medical information can be given. It merely found that the government satisfied each factor. *See id.*

78. *See id.*

79. *See id.*

80. *See id.*

81. *See id.* at 579.

82. *See id.* at 580.

83. *See id.* Specifically, the study distributed to employees and others included only aggregate data. NIOSH kept the data it retained in locked cabinets in locked rooms. Material from smaller studies was not placed on computers, and data from large studies were removed

indicate that each of the seven factors had to be met in order to prove that the employee's rights had been violated; rather, the court merely found that the government satisfied each component.[84]

Westinghouse nonetheless created a paradigm for determining when an intrusion into private medical records rises to the level of a constitutional violation. The decision also exemplified the deference given to governmental interests in such cases, even in light of an acknowledged constitutional right to privacy.

In 1995, the Third Circuit again applied the *Westinghouse* seven factor test in *Doe v. Southeastern Pennsylvania Transportation Authority ("SEPTA").*[85] In *SEPTA*, the court held that the Southeastern Pennsylvania Transportation Authority's inadvertent discovery and minimal disclosure of the plaintiff's medical prescription records did not violate his constitutionally protected right to privacy.[86]

SEPTA discovered that the plaintiff had AIDS from a pharmacy report containing the plaintiff's name and medical prescription information.[87] Doe subsequently brought suit, alleging that the discovery of his condition violated his right to privacy.[88]

The *SEPTA* court first reasoned that the limited right to privacy in personal medical records generally includes medical prescription records, because people using prescription drugs legitimately expect this information to remain private.[89] The court then applied the *Westinghouse* balancing test to determine whether the disclosure of Doe's prescription information constituted a violation of his constitutionally protected right to privacy.[90] The court found that the minimal intrusion upon Doe's privacy was insufficient to

---

from computer storage after six months. When outside contractors compiled similar data, they were contractually bound to a policy of nondisclosure. *See id.*

84. *See id.* at 578.

85. Doe v. SEPTA, 72 F.3d 1133, 1140 (3d Cir. 1993).

86. *See id.* at 1134.

87. *See id.* at 1135-36. Although SEPTA did not routinely request patient identification information on these reports, SEPTA's pharmacy submitted a report to SEPTA's Chief Administrative Officer containing the names of employees who had obtained prescription medication costing more than $100 in the previous month. *See id.* at 1135. When the Chief Administrative Officer and Director of Benefits reviewed the pharmacy report and were unable to identify one of Doe's prescribed medications, they contactod a SEPTA staff physician and Doe's doctor to determine the drug's use. *See id.* In doing so, they discovered that Doe had AIDS. *See id.*

88. *See id.* at 1134-35. Doe did not allege any injury other than the intrusion into his private medical information. *See id.*

89. *See id.* at 1138.

90. *See id.* at 1139-40.

require SEPTA to prove it had a compelling interest in obtaining the information.[91]

The lone dissent predicted that the court's decision would "make it far easier in the future for employers to disclose their employee's private medical information . . . and to escape constitutional liability."[92] In the majority opinion, however, such reservations were insufficient to overcome the strong state interest in disclosure.[93]

In stark contrast to the Third Circuit's comprehensive exploration of the constitutional zone of privacy surrounding medical records and prescription information, the Sixth Circuit, in 1995, summarily held that the Constitution does not provide a general right to nondisclosure of private information.[94] Rather, the court stated that "inferring very broad 'constitutional' rights where the Constitution itself does not express them is an activity not appropriate to the judiciary."[95] The Sixth Circuit has held that unwarranted disclosure of medical information does not violate the Constitution because such disclosure fails to infringe upon a "fundamental right," and thus the court should not be involved.[96]

Most recently, in 1999, the Fourth Circuit noted the conflict over whether an individual possesses a constitutional right to privacy in medical records, but declined to definitively decide the question.[97] Implicitly adopting the *Westinghouse* balancing test but failing to apply it in a constitutional context, the *Ferguson v. City of Charleston* court concluded that "even if Appellants possess a constitutional interest in the nondisclosure of their medical records, that interest is outweighed by the interest of the government in disclosure."[98]

---

91. *See id.* at 1140.

92. *Id.* at 1147 (Lewis, J., concurring in part and dissenting in part).

93. The court stated:

> We hold that a self-insured employer's need for access to employee prescription records under its health insurance plan, when the information disclosed is only for the purpose of monitoring the plans by those with a need to know, outweighs an employee's interest in keeping his prescription drug records confidential. Such minimal intrusion, although an impingement on privacy, is insufficient to constitute a constitutional violation.

See id. at 1143

94. *See* Jarvis v. Wellman, 52 F.3d 125, 126 (6th Cir. 1995).

95. *Id.* (citing J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (concerning an unauthorized disclosure of a prison inmate's medical records to her father, who was also an inmate at the same prison)).

96. *See id.* at 126.

97. *See* Ferguson v. City of Charleston, 186 F.3d 469, 482-83 (4th Cir. 1999).

98. *Id.* at 483.

At present time, it appears that judicial formulations will rarely, if ever, allow individual privacy interests to trump the government's interest in disclosure. Moreover, even if these judicial tendencies shifted in favor of personal privacy, there are still additional limitations that would severely curtail the effectiveness of a general constitutional protection of information privacy.

D. Fundamental Limits to the Constitutional Solution: State Actors and the Private Medical Profession

Even if the United States Constitution were interpreted to protect privacy rights in medical records, it would only apply to records held by the government.[99] Despite this limitation, a recent study reported in *Harper's Magazine* found that more people were concerned about government access to private information than access to such information by private companies.[100] This indicates that a constitutional solution could indeed protect private information from an entity that many people perceive as the greater threat to their privacy.

Nonetheless, this potential solution ignores the reality that medical care has become increasingly privatized, thus rendering a constitutional privacy protection of medical records less potent.[101] Thus, although the Constitution may, in fact, offer a partial solu-

---

99. As one commentator notod:

> [T]he constitutional right to privacy does not provide reliable protection for medical data. *Whalen* has never been applied to provide protection to computerized health information. In addition, *the constitutional right to privacy is limited to state action; therefore, unless the government is the collector or disseminator of the information, one must look elsewhere for protection of this information.*

See, e.g., Carter, *supra* note 2, at 241 (emphasis added).

100. *See* Forum, *The Searchable Soul: Privacy in the Age of Information Technology*, HARPER'S, Jan. 2000, at 59 [hereinafter *The Searchable Soul*]. Alan Westin, Professor Emeritus of Public Law and Government at Columbia University, supplied this information as part of a forum discussion reprintod in *Harper's*. *See id.* at 58. Westin was instrumental in the passage of the Federal Privacy Act of 1974. *See id.*

101. "One sobering outcome of these economic reform measures has been a radical shift in the role of the state. Where the state once assumed responsibility for providing public services such as health, education, or transportation, the trend now is towards deregulation and privatization." *See* Symposium, *Markets and Women's International Human Rights*, 25 BROOK. J. INT'L. L. 141, 145-46 (1999). One commentator has noted how the private sector has gradually become an increasing threat to individual privacy, gradually taking over the role of the government as the biggest perceived threat to such mattors. *See* Gellman, *supra* note 23, at 209. Another drawback of a constitutional solution is its remedy. When suing under a constitutional theory, the best remedy available for a plaintiff is injunctive relief, which remains insufficient in many cases. *See id.*

tion to the problems surrounding medical information privacy, such a solution remains inadequate in a modern context.

III. LEGISLATIVE AND REGULATORY ATTEMPTS TO PROTECT MEDICAL RECORDS PRIVACY

Like the problems that plague a possible constitutional protection of private medical records, legislative and regulatory models also are wrought with difficulties. Because federal legislation offers protection for medical records based on the characteristics of the entity seeking access, it provides only a fragmented and unsatisfactory solution on its own. Likewise, state legislation has similar problems, and state legislators face the additional, perhaps insurmountable, difficulty of not having any real impact on medical information that crosses state lines, because this information is considered interstate commerce.

A. The HHS Regulations

The issue of medical records privacy is receiving increased legislative and regulatory attention. On October 29, 1999, President Clinton proposed broad medical privacy regulations that controlled access to medical information stored in an electronic medium.[102] These regulations would require doctors, hospitals, and health plans to seek and obtain written consent from patients before releasing personal information for purposes not related to payment and treatment.[103] These regulations apply only to electronic records, however, and do not give patients a right to sue their medical providers.[104] Instead, the HHS would bring lawsuits for violations of the regulations.[105]

Critics of the proposed regulations point out that law enforcement officials would not be required to comply with the terms

---

102. *See* Declan McCullagh, *New Medical Privacy Mandate* (last modified Oct. 29, 1999) <http://wired.com/news/politics/0,1283,32209,00.html>. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Congress gave itself a deadline of August 21, 1999 to create confidentiality legislation or defer to HHS to develop privacy protections. After Congress missed the deadline, President Clinton announced the proposed HHS rules, but encouraged Congress to continue attempting to pass legislation due to the shortcomings of a regulatery solution. *See* Rebecca L. Jackson, et al., *Federal Legislation to Protect Patient Confidentiality not Expected Before Fall*, 7 METRO. CORP. COUNS. 15 (Aug. 1999); President William J. Clinton, Remarks on medical privacy, Nov. 1, 1999, *in* M2 Presswire, *available in* 1999 WL 24365495.

103. *See* McCullagh, *supra* note 102.

104. *See id.*

105. *See id.*

of the regulations, and the regulations do not restrict the activities of lawyers, auditors, or consultants who come in contact with private medical information.[106] Furthermore, some free market groups argue that the complex proposal is "too regulatory," fearing that the cost of medical insurance could increase because of the additional red tape.[107] Still other critics express dissatisfaction with the proposed rules because they claim that President Clinton has overstepped the bounds of his constitutional authority in regulating an issue that is better left to Congress.[108] Finally, some observers criticize the regulations themselves. When HHS Secretary Donna Shalala described her attempt to "balance the protection of privacy with our public responsibility to support national priorities," skeptics noted that this process was significantly less stringent than the "compelling public interest" test typically employed in the judicial context.[109] According to one commentator, the regulations essentially grant law enforcement officials unlimited access to examine anyone's medical records without sufficiently limiting their access or dissemination of the information.[110] From this perspective, the proposed regulations contain the same problems that plague the constitutional solution—too much deference to the government's interest in disclosure.

Significantly, the proposed regulations failed to impress those upon whom they would have the greatest effect, namely doctors and insurance companies. A recent article outlined the dissatisfaction of both groups.[111] Doctors were unhappy with a provision allowing managed care plans to use personal information without consent if the purpose was "healthcare operations."[112] This language, physicians argued, constituted a loophole through which HMOs and other insurers could pry into the doctor-patient relationship under the guise of assessing the quality of care.[113] Similarly, insurers

106. *See* Shailagh Murray, *Clinton to Propose Regulations Today to Protect Privacy of Medical Records*, WALL ST. J., Oct. 29, 1999, at A4.

107. McCullagh, *supra* note 102.

108. *See* Michael Posner, *Blocking the Presidential Power Play*, NAT'L. L.J., Jan. 1, 2000 ("Presidents have broad authority under the Constitution to issue orders to run the executive branch, but . . . others contend that Presidents since Theodore Roosevelt—especially Clinten—have stretched, if not abused, their powers by taking over the authority of Congress to legislate.").

109. SYKES, *supra* note 3, at 116-17.

110. *See id.* at 117 ("Indeed, [Shalala's] proposal would have made it easier for investigaters to get someone's medical records than to get records about their movie rentals or cable television habits—all protected by federal law.").

111. *See* Evan Thomas, *A Question of Privacy*, NEWSWEEK, Nov. 8, 1999, at 67.

112. *Id.*

113. *See id.*

pointed to a provision holding them liable for privacy breaches by "business partners" such as lawyers and accountants, arguing that the rules would make them too vulnerable to lawsuits.[114]

In addition, both physicians and insurers agreed that privacy protections would drive up the cost of health care by more than $3.5 billion over the next five years.[115] Both groups also complained about the increased level of federal scrutiny required by the new rules' enforcement provisions.[116]

Because of the widespread criticism of the regulations and the practical difficulties that would arise in implementing them, they appear to be, at best, a temporary solution that will remain in place until a better measure of protection can be implemented.

B. The Privacy Act of 1974

In addition to the regulations imposed by HHS and President Clinton, a number of other federal legislative solutions have existed in various forms since 1974. The Privacy Act of 1974 attempts to ensure that "the government will use fair information practices with regard to the collection, use and dissemination of individually-identifiable records."[117] The Act mandates that government agencies not disclose "any record" that exists within a "system of records" controlled by a government agency.[118] When agencies do collect data, they must notify the individual that data is being collected and the reason for its collection.[119]

The Privacy Act allows for civil remedies, and, in some cases, criminal penalties, if a disclosure is made in willful contravention of the Act.[120] The chief limitation on the effectiveness of the Privacy Act lies in the numerous exceptions that severely weaken its overall

---

114. *Id.*

115. *See id.*

116. *See id.*

117. Carter, *supra* note 2, at 241 (citing The Privacy Act of 1974, Pub. L. No. 93-579, §1, 88 Stat. 1896 (codified as amended at 5 U.S.C. §552a (1994)). Carter notes that the Computer Matching and Privacy Protection Act amended the Privacy Act in 1988. The Computer Matching and Privacy Protection Act regulates the "matching" of files by using an individual's personal identifier, such as a social security number. *See id.* at n.96 (citing Pub. L. No. 100-503, 102 Stat. 2507 (amending 5 U.S.C. §552a (note)).

118. *Id.* at 242.

119. *See id.*

120. *See id.* (citing 5 U.S.C §552, which provides tbat employers or officers who willfully disclose confidential information to any person or agency not entitled te receive such information will be guilty of a misdemeanor and subject te a maximum fine of $5000).

impact.[121] For instance, no patient consent to disclosure is necessary if an agency decides to make disclosure for "routine uses," reasons "compatible with the uses for which the data was collected."[122] Still further, the Act provides no protection for privately held information.[123]

C. The Freedom of Information Act

The Freedom of Information Act ("FOIA")[124] requires that "information held by executive branch agencies be made available on request to the general public," subject to exemptions which "may allow a government agency to withhold medical information requested under FOIA."[125] Moreover, information that must be disclosed under FOIA is not protected by the Privacy Act, thus further limiting the Act's effectiveness.[126]

In summary, although existing and proposed federal legislation may provide comprehensive protection of records held by government entities, it covers very little else. Like the aforementioned various constitutional solutions, the federal regulatory responses impose virtually no restrictions on what private healthcare providers may disclose to third parties. Moreover, rules that do protect privately held information, like the HHS regulations, are seriously limited in other ways, as, for example, the existing battle over whether federal legislation might actually erode protection of private medical records by preempting tougher state laws demonstrates.[127] As discussed below, similar defects plague state attempts at privacy legislation.

---

121. *See id.* at 242-43.

122. *Id.* at 243.

123. *See id.* The net result of the Privacy Act is, then, that, while federally operated hospitals and private healthcare facilities under contract with the federal government are covered by the Privacy Act, other institutions—such as those that are exclusively private—are not.

124. 5 U.S.C. §552 (1994).

125. Carter, *supra* note 2, at 244. Exemption six of the FOIA "pertains to 'personnel and medical files . . . the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.' " *Id.* This exemption operates to "prevent disclosure of individually-identifiable medical information, unless there is a public interest which outweighs the privacy interest in nondisclosure." *Id.*

126. *See id.* (citing 5 U.S.C. § 552(b)(2)).

127. *See supra* Part III.A. An additional fear about federal legislation is that it would preempt more restrictive state laws. As a long-term strategy, however, state-by-state regulation of privacy is not compatible with modern methods of healthcare delivery. *See* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 516 (1995). Nevertheless, at least one commentator recommends maintaining state protections until a federal solution can be found in order to avoid situations that will sacrifice patient rights. *See* Carter, *supra* note 2, at 285.

D. State Attempts at Privacy Regulation

Traditionally, health care has been subject to state regulation.[128] Several states provide constitutional protections for individual privacy interests.[129] Like the Federal Constitution, however, state constitutional protections are inherently weak in that they protect only against invasions of privacy by state actors.[130] In addition, state constitutions offer no satisfactory remedies unless "the state fails to assert any significant interest or is particularly careless in disclosing highly sensitive information."[131]

Protection of individual privacy may also be achieved under state common law.[132] Tort actions for privacy invasions or suits based on an implied contract between doctor and patient are possible remedies in some cases.[133] Critics argue that tort remedies are not useful for individuals, however, because the relief available "will not meet the broad objectives of the code of fair information practices."[134] For example, privacy tort law provides no liability for the use of public record information, and common law extension of this rule by judges remains unlikely since tort directives are statutory in nature and many judges are reluctant to enter into this area of judicial decision-making.[135] State common law protections are weak because they are often ineffective in cases involving medical records since the majority of medical records travel in interstate commerce. As such, these records become subject to federal—not state—regulation. In addition, many states do not recognize the

---

128. *See* Carter, *supra* note 2, at 245.

129. *See id.* at 246 & n.131. These states include Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. *See id.*

130. *See id.* Carter points out a provision in the California Constitution that extends the state constitutional right to privacy to private entities in addition to the government, but this is a rare exception. *See id.* at 254.

131. *Id.* at 246-47 (quoting Gostin, *supra* note 127, at 498 & n.211).

132. *See id.* at 247.

133. *See id.* at 248. Carter notes the argument for implied contract as one where:

> "[a]ny time a doctor undertakes the treatment of a patient, and the consensual relationship of physician and patient is established, two jural obligations . . . are simultaneously assumed by the doctor. Doctor and patient enter into a simple contract . . . . As an implied condition of that contract . . . the doctor warrants that any confidential information gained through the relationship will not be released without the patient's permission."

Id. at 248-49 (quoting Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 801 (N.D. Ohio 1965)). Defamation suits may be brought in some states "if medical data containing inaccurate information are disclosed to an unauthorized person, and if the subject's reputation is adversely affected." *Id.* at 249 (citation omitted).

134. Gellman, *supra* note 23, at 210.

135. *See id.* at 211.

above-mentioned tort privacy causes of action.[136] Consequently, numerous states have enacted legislation to fill the gap left by insufficient state common law protections.[137]

Privacy legislation exists in every state that requires some level of reporting of patient information to public health or law enforcement agencies.[138] Similarly, most states recognize that information shared between patient and physician is privileged, although at least one critic has argued that this privilege protects only against disclosure of confidential medical information in judicial proceedings.[139]

Like any legislation, there are limits to the effectiveness of state laws governing the privacy of medical records. For example, some states protect only medical information related to certain sensitive diseases, such as HIV or mental illness.[140] In addition, state legislation typically conditions privacy protection on the party holding the information, and not on the type of information held.[141] Some of the more comprehensive statutes, such as one in New York,

---

136. Carter argues:

> Under one or a combination of these tort causes of action, a patient may recover damages for the improper release of confidential medical information. However, as noted, these claims are often ineffective in medical records cases, and the causes of action are not recognized in all states. As a result, many states have passed legislation to address some of these confidentiality issues.

Carter, *supra* note 2, at 249

137. *See id.* at 249-50. According to Carter, about 20% of the states have such legislation. *See id.* Many of these statutes are based on the Federal Privacy Act of 1974, *see supra* noto 117, and provide a degree of assurance that medical data held by the state will not be disclosed to third parties without the patient's consent. *See* UNIF. HEALTH CARE INFORMATION ACT, prefatory note, 9 U.L.A. 475-76 (1998) (citing data practices statutes from eight states as examples); *see also* Harris, *supra* note 3, at 1212-13 (noting that Arizona, California, Montana, and Rhode Island have also enacted comprehensive legislation to protect healthcare information).

138. *See* UNIF. HEALTH CARE INFORMATION ACT, prefatery note, 9 U.L.A. 475-76 (1998). Note that, if information is passed on to state agencies such as public health or law enforcement agencies, a constitutionally recognized protection of privacy would prevent disclosure from these agencies to third parties.

139. *See* UNIF. HEALTH CARE INFORMATION ACT, prefatery note, 9 U.L.A. 475-76 (1998). This provision exists only if it is decreed by statutes, since there was no physician-patient privilege at common law. *See id.*; *see, e.g.*, MICH. COMP. LAWS § 600.2157 (1986 & Supp. 1998) ("[A] person duly authorized to practice medicine or surgery shall not disclose any information that the person has acquired in attending a patient in a professional character, if the information was necessary to enable the person to [treat] the patient as a physician . . . .").

140. *See, e.g.*, CONN. GEN. STAT. ANN. § 19a-584 (West 1997); IDAHO CODE §39-610 (1998).

141. *See* Carter, *supra* note 2, at 251 (footnote omitted).

impose a duty of confidentiality on non-provider parties[142] like insurance companies.[143]

The most restrictive limitation of state legislation is lack of consistency among states.[144] When medical information travels between states, as is often the case with Internet, telephone, or facsimile transportation of information, no state law will protect the confidentiality of that information.[145] State protections, therefore, no matter how stringent, will not protect the privacy of medical records transferred over the Internet.

IV. SELF-REGULATION: A MATTER OF INCENTIVE

With the rapid growth of the Internet and the absence of other effective means of protection, many companies have implemented their own privacy policies in order to protect their clients'

142. For purposes of this Note, "non-provider" parties refers to parties other than the entity providing healthcare. Examples of non-provider parties include insurance companies and research facilities.

143. *See* Carter, *supra* note 2, at 251 (citing Lawrence O. Gostin et al., Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, pt. 4, § II.A. (Feb. 1997)).

144. *See id.* at 253-65 (summarizing the legislation in effect in California, Tennessee, and Minnesota); *see also* Glenn R. Simpson, *E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise*, WALL ST. J., Jan. 6, 2000, at A24 (noting that pending legislation exists in California to prohibit Internet service providers from disclosing personal information without customer permission and to create an office of the "Privacy Ombudsman" to investigato the unlawful release of personal information by commercial or governmental entities and to allow civil suits for unlawful release of personal information). In addition, pending legislation in New York would establish an opt out systom for unsolicited marketing, restrict collection, disclosure, and dissemination of personal information, and enact a tolecommunications privacy law regulating the collection, use, or disclosure of information by telecommunications carriers. *See id.* (citation omittod).

145. *See id.* at 265; *see also* ACLU v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999) (quoting American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997) (agreeing tbat "[t]he unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however is a virtually meaningless construct on the Internet."). The *ACLU v. Johnson* court also supported the notion that there is no such thing as *intrastate* commerce over the Internet since Internet speech is available in any location and that state laws regulating the Intornet "cannot effectively be limited to purely *intrastate* communications over the Internet because no such communications exist." *Id.* (quoting *Pataki*, 969 F. Supp. at 171 (emphasis added)); *see also* United States v. Whiting, 165 F.3d 631, 634 (8th Cir. 1999) (noting that the downloading of Intornet images onto a personal computer requires the use of interstate commerce); United States v. Simpson, 152 F.3d 1241, 1245 (10th Cir. 1998) (noting the use of interstate commerce in transferring files via the Internet).

and customers' interests.[146] Self-regulation, though, is not limited to Internet transactions. The securities industry, for example, has regulated itself on-line as well as on paper.[147] Many advocates argue that such a scheme would best protect electronically stored medical information.[148] Indeed, President Clinton's top Internet adviser, Ira Magaziner, observed in 1998 that "private industry must respond to growing public concerns about issues such as privacy in the digital age and that businesses and consumer groups must work together to develop industry standards that protect privacy."[149] Similarly, Lori Fena, chairwoman of the Electronic Frontier Foundation, noted that self-regulation is most effective when accompanied by "a huge threat of legislation" as well as by marketplace incentives.[150]

Moreover, since medical records have economic value, members of the business community fear that stringent legislation might stifle legitimate e-commerce.[151] One author suggests that the creation of successful and enforceable fair information practices may be a matter of establishing effective and appropriate incentives.[152] In the past, policies implementing the principles of information privacy have not included the types of incentives necessary

146. Other attempts to control access te private medical information have resulted in small-scale attempts by those in the medical services industry to police themselves when transmitting medical information electronically. *See* Ann Carrns, *Intel and AMA Form Service to Improve Security of Online Medical Information*, WALL ST. J., Oct. 12, 1999, at B6.

147. *See generally* DAVID P. MCCAFFREY & DAVID W. HART, WALL STREET POLICES ITSELF (1998) (providing an overview of the self-regulatory mechanisms at work in the securities industry–under the federal securities laws, the national securities exchanges, registered securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board have the power to creato rules, with the SEC's approval, that encourage fair, ethical, and efficient practices in the securities industry).

148. *See White House's Magaziner advises Internet self-regulation*, The Freedom Forum Online (last modified Jan. 13, 1998), <http:// freefomforum.org/technology/1998/1/13magaziner.asp>.

149. *Id.*

150. *Self-Regulation Needed to Ensure Privacy*, TechWeb (last modified Mar. 13, 1998), <http:www.techweh.com/wire/story/TWB19980313S0018>. For a discussion of marketplace incentives, see *infra* Part IV.A.

151. *See* Steve Zurier, *Privacy Sound Off: Regulation vs. Self-Regulation* (last modified Sept. 21, 1998), <http://www.internetwk.com/trends/trends092198.htm> ("[Self-regulation] mean[s] letting the private sector lead the way in making online transactions secure so that e-commerce can be conducted safely, and offering consumers options so that their confidence in online commerce can be won and maintained.").

152. *See* Gellman, *supra* note 23, at 213 ("Privacy principles have generally not been implemented in ways that offer natural incentives to record keepers to comply. Few existing legal devices have proved effective in pressuring record keepers to take affirmative steps to meet privacy objectives. If adequate pressure or interest exists, any of the devices might work.").

to induce record keepers to comply.[153] As a result, existing legal devices are ineffective in pressuring record keepers to take affirmative steps to meet privacy objectives.[154] If adequate incentives are applied, however, any of the devices may work.[155] One such incentive may be marketplace competition; another might be the threat of tough federal legislation and enforcement.

A. The Marketplace Incentive

According to one commentator, the marketplace is the most powerful incentive for regulating business on-line: "Self-regulation works according to the law of customer satisfaction. Without this satisfaction, there can be no consumer confidence, no online transactions and certainly no thriving Internet marketplace, as exists today."[156]

One way to create such an incentive may be to create specific privacy codes that could be jointly adopted by merchants and consumers and enforced through private mechanisms.[157] But for this to work, merchants and consumers must provide adequate interest in enforcement mechanisms.[158]

The effect that marketplace incentive has on companies that maintain private information in electronic storage is already clear in a few instances. For example, when America Online saw its stock price drop after announcing it planned to sell user information, the

---

153. *See id.*

154. Some legal scholars argue that privacy matters are not for the judiciary or legislature to decide. One commentator has stated that privacy matters "concern decisions that should not be made by any governmental body or official, but should be left to individuals." *See* Strossen, *The Right to Be Let Alone: Constitutional Privacy in* Griswold, Roe *and* Bowers, *in* BENCHMARKS: GREAT CONSTITUTIONAL CONTROVERSIES IN THE SUPREME COURT 90 (Terry Eastland ed., 1995). But for individual decisions to have any ascertainable effect on medical records privacy, the level of interest among individuals must be high. *See id.*

155. *See id.*

156. H. Robert Wientzen, *Privacy Sound Off: Self Regulation* (last modified Sept. 21, 1998), <http://www.internetwk.com/trends/trends092198-2.htm>. One way to implement such a model is to post privacy policies and let customers decide whether to use a particular storage format, health care provider or insurance company based on what kind of access will be available. This would be possible for records stered on paper as well, but this option is weakened by the fact that, under many managed care programs, patients do not have much choice of who their healthcare or insurance providers will be. Still, companies do have this choice, and arguably have more influence on the marketplace than individuals, thus potentially making the effectiveness of the marketplace incentive stronger.

157. *See id.*

158. *See id.*

company quickly abandoned the idea.[159] Similarly, when asked how best to protect electronically stored private information, Alan Westin, Professor Emeritus at Columbia University and key player in the passage of the Privacy Act of 1974, responded that the best way to protect against the unwarranted release of private information is,

> [b]y the perception of the marketplace and because of the privacy advocates' vigilance. When a [banking] conglomerate . . . was formed, they issued a privacy promise, which they registered with the federal regulators as well as posted on their Web site, that said: "We will never use health information from our [health insurance] subsidiary for any situation that has to do with banking or financing." Now, why did they do that? They did it as self-denial, they would have loved to put that information together. They did it because of the perception that they would not have happy customers if they used people's health information that way.[160]

Several companies, weary of waiting for federal legislation to take over, have already implemented their own privacy strategies.[161] For instance, Intel and the American Medical Association announced in October 1999 that they would offer an on-line service to provide a means to "authenticate the identity of doctors seeking to access and transmit health data in cyberspace . . . . Boosting security is seen as key to the widespread adoption of Internet based medical transactions, which have the potential to reduce paperwork and cut costs."[162] The marketplace incentives could provide additional protection for medical records privacy, but not without stronger consumer interest and awareness of the privacy issue.

B. The Threat of Federal Regulation as an Incentive to Self-Regulate

As noted above, other industries have implemented a self-regulatory regime with a considerable degree of success.[163] Two commentators note that the term "self-regulation" understates how much its effectiveness depends on government agencies and the in-

---

159. *See Self-Regulation Needed To Ensure Privacy*, TechWeb (last modified Mar, 13, 1998), <http:www.techweb.com/wire/story/TWB19980313S0018>.

160. *The Searchable Soul*, *supra* note 100, at 66. Ron Sege, executive vice president of Lycos, noted that the reason for privacy policies on the Internet, including the Lycos privacy policy, is "[b]ecause I believe it will maximize the value of the firm over the long term. And if I start selling this information, then customers are going to go someplace else." *Id.*

161. *See* Carrns, *supra* note 146; *HP Calls for Self-Regulation to Address Online Privacy* (last modified June 23, 1998), <http://www.hp.com/latinamerica/mpg/html/privacy.html>.

162. Carrns, *supra* note 146, at B6.

163. *See generally* MCCAFFREY & HART, *supra* note 147, at 6-8, 176-87 (defining self-regulation and discussing its usefulness in various industries).

fluence of other disciplinary bodies.[164] Similarly, "[s]elf-regulatory organizations and firms have room to design regulatory systems rather than having to implement rules designed largely by the government, and the right to largely control themselves is theirs to lose."[165]

In a survey of the self-regulatory efforts of the securities industry, commentators looked at several case studies involving attempts at self-regulation in other industries.[166] One study of the operations of pharmaceutical companies reported that internal quality control resulted in collection of better information about cooperation with company policy than external regulations.[167] This resulted in more effective detection of problems.[168] Specifically, the self-regulating systems proved more effective than government regulation where the threat of liability, bad press, or the potential for Food and Drug Administration ("FDA") actions existed. These external pressures helped convince top level management to comply with the self-policing rules.[169]

The authors of the survey argue that self-regulation is most effective when it exists alongside the threat of external regulation.[170] They stress that neither public nor private systems of regulation are intrinsically superior.[171] Instead, they point out that the notion that government regulation is more stringent than private regulation (and thus should serve as a baseline to measure private regulation's performance) oversimplifies the issue.[172] The distinct advantage of public regulation, they argue, is that it is relatively independent of the advocates of production and therefore less likely to be excessively permissive.[173] This remoteness, however, leaves public regulators less informed and often unable to handle situations effectively.[174] In comparison, private regulators, such as internal quality control programs and specially trained staffs who exist to ensure compliance, are better informed and more

164. *See id.* at 7.
165. *Id.*
166. *See id.* at 180.
167. *See id.*
168. *See id.*
169. *See id.*
170. *See id.* at 183.
171. *See id.*
172. *See id.*
173. *See id.*
174. *See id.*

adaptable, but they may not be self-sufficient.[175] Thus, both private and public regulatory bodies are necessary to make self-regulation most effective.

C. Problems with Self-Regulation

The concept of self-regulation as the best means of protecting the privacy of electronically stored personal information is not without its critics. In 1997, the Federal Trade Commission agreed to a self-regulation plan offered by 14 data collection agencies, which together account for roughly 90% of the personal information retrieval business.[176] Since its inception, however, the mechanics of this program have raised doubts among privacy advocates.[177] For example, the plan requires individuals to opt out of databases by actively requesting that third parties receive limited access to personal information.[178] Critics argue that "[m]any people don't even know that these entities exist," and that such restrictions are only "cosmetic."[179] As criticism has mounted, the electronic-commerce industry has softened its opposition to federal regulation of Internet privacy issues.[180] One past advocate of self-regulation even observed that "[s]ome in the industry are mulling whether we're not better off working at a federal level to create some standards."[181] Although proponents of self-regulation have argued that new legal restrictions could hinder the commercial growth of the Internet,[182] multiplying reports of surreptitious collection of consumer data by Internet marketers and questionable distribution of such personal data by other companies make privacy an issue of increasing public concern.[183]

In the 2000 presidential primaries, both Vice President Albert Gore and Republican Steve Forbes jumped on the issue.[184]

---

175. *See id.* McCaffrey and Hart point out that external regulation, private legal action and political and economic pressures often produce undesirable outcomes such as waste, but self-regulation does not work effectively without them. *See id.* at 184.

176. *See FTC Gambles on Internet privacy* (visited Jan. 28, 2000), *available in* <http://www.main.nc.us/FTC/>.

177. *See id.*

178. *See id.*

179. *Id.*

180. *See* Simpson, *supra* note 144, at A24.

181. *Id.*

182. *See id.*

183. *See id.*

184. *See id.* For example, Steve Forbes said in a speech to the Free Congress Foundation that "[p]rivacy is the basis for a free society . . . . The biggest and most serious threat to our

Meanwhile, lawmakers from both parties are calling for safeguards such as requiring companies to disclose how they collect data and use personal information, and to obtain consumer permission before they resell the data.[185] Other executives continue to look to the market as the primary solution to the problem but remain prepared to work with Congress if self-regulation does not prove a workable model for protecting medical records privacy.[186]

V. CONCLUSION

Despite these legitimate concerns, many legal scholars insist that personal information privacy is an area "where Internet self-regulation works best."[187] For example, according to Michael Moynihan, former member of the Treasury and Commerce Departments and principal architect of the Clinton Administration's Internet regulation policy, it is overly optimistic and unrealistic to believe in the government's ability to solve the problem of Internet privacy invasions.[188] "Even if legislation is passed to deal with the most problematic areas, health records, for example, the underlying trend is for information to become more and more accessible. Government won't deal with that."[189] Even if it does, there are limits as to what records and what record keepers the government can regulate.

Similarly, the National Research Council warns that medical records are especially vulnerable to abuse since "there are no strong incentives to safeguard patient information because patients, industry groups and government regulators aren't demanding protection."[190]

This lack of incentive remains perhaps the biggest limit on self-regulation. According to Bill Hogan of the Center for Public Integrity, "[t]here is no real money constituency in favor of privacy,

---

privacy comes from a massive federal government seeking information it does not need, nor a constitutional right to have." Godfrey, *supra* note 52, at A8.

185. *See id.*

186. *See id.*

187. PRESTON R. PADDEN, CYBERLIABILITY, 582 PLI/Pat 7, *9 (1999) (on file with author).

188. *See The Searchable Soul*, *supra* note 100, at 64.

189. *Id.* In his final State of the Union Address, President Clinton addressed this problem by noting the recent regulations, but qualifying them with the statement that achieving compromise in Congress will be difficult in this era of third-party payers and external review of medical decision-making. *See* Rick Green & Andrew Julian, *State of the Union*, HARTFORD COURANT, Jan. 28, 2000, at A14, *available in* 2000 WL 4224778.

190. SYKES, *supra* note 3, at 118.

and there is a lot of money in favor of invading it."[191] Still, despite these concerns, self-regulation remains far from a futile proposition. If sufficient interest, incentives and enforcement mechanisms can come to fruition, then a functioning marketplace and the threat of restrictive governmental intervention could spur the creation of satisfactory modes of protecting medical records privacy. Free from the problems of other modes of regulation, self-regulation is worth the effort it will take.

Catherine Louisa Glenn[*]

191. *Id.* at 119.

* I am indebted to my friends and editors, Stephanie Blackman and Robert Roos, for their careful eyes and helpful suggestions. Thanks also to Mike Bronson for his attention to the bottom half of this Noto. Finally, I owe much gratitude to my parents and sister, for their love and support throughout my education, and to my friends, Erin Connolly and Kerry Ducey, who have made law school a better place.