UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 4 *Journal of Computer & Information Law - Summer 2001*

Article 1

Summer 2001

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 (2001)

Kevin B. Davis

ARTICLES

PRIVACY RIGHTS IN PERSONAL INFORMATION: HIPAA AND THE PRIVACY GAP BETWEEN FUNDAMENTAL PRIVACY RIGHTS AND MEDICAL INFORMATION

KEVIN B. DAVIS†

I. INTRODUCTION

Every technological advancement brings with it unintended consequences—some good, some not so good.[1] With regard to health issues, developments of computer technology have impacted nearly every facet of health care,[2] from diagnosis to treatment to administration. Information about a patient—such as a digital image of an x-ray or remote monitoring of vital signs—can be quickly accessed by physicians at nearly anytime and in nearly any location, thus providing physicians with potentially crucial information to aid in patient care.[3] This is the good. The not so good is that the same information, and more, such as how many days overdue a payment is, or the results of sensitive medical

† Kevin Davis is an attorney in New York. His practice emphasizes technology, privacy, and corporate matters. He received his B.A. from Michigan State University; M.A. from American University, and J.D. from the University of Denver College of Law. This Article is dedicated to Lisa and Nathan, for the endless support and inspiration each provides. For more information, or to contact the author, please visit www.DavisEsq.com.

1. *See e.g.* Bill Joy, *Why the Future Doesn't Need Us*, Wired (Apr. 2000) (available at <http://www.wired.com/wired/archive/8.04/joy.html>). Joy was cofounder and Chief Scientist of Sun Microsystems. *Id.*

2. *See generally* Smart Communities, *Building Smart Communities: A New Framework for an Americas Information Initiative*, Address by John M. Eger to the International Telecommunication Union Americas Telecom '96, Rio de Janeiro, Brazil (June 10-15, 1996) (available at <http://www.smartcommunities.org/library_newframe.htm>).

3. *See generally* Adam William Darkins & Margaret Ann Cary, *Telemedicine & Telehealth* (Springer Publg. Co. 2000).

tests, are equally accessible.[4] As the amount of people with access to medical information of a sensitive nature has grown, those in the medical community and privacy advocates began to recognize the need for broad privacy protections to medical data. The result of this campaign is the *Standards for Privacy of Individually Identifiable Health Information* (the "Privacy Rule"), a set of regulations promulgated by the Secretary of Health and Human Services ("HHS").[5] The Privacy Rule was required by the *Health Insurance Portability & Accountability Act of 1996* ("HIPAA"), then popularly known as the *Kennedy-Kassenbaum Act*.[6] At the time, HIPAA received significant attention, because it made it easier for an employee to maintain health insurance after leaving a job.[7] HIPAA also provided that if Congress did not pass legislation pertaining to medical privacy within a specified time, HHS would promulgate regulations to that affect.[8] HHS issued a proposed rule in October 1999, and after an unusually long and contentious comment period and a clerical error that nearly derailed the regulations at the last second, the Privacy Rule was implemented in early 2001.[9] The Privacy Rule pro-

4. The Supreme Court has recognized the potential for abuse of large amounts of information kept in databases, saying, "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive governmental files." *Whalen v. Roe*, 429 U.S. 589, 605 (1976).

5. *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164 (2000)) [hereinafter Standards]. On July 6, 2001, HHS released a "Guidance" for the Regulations. HHS, *HHS Issues First Guidance on New Patient Privacy Protections* ¶ 1 <http://www.hhs.gov/news/press/2001pres/20010706a.html> (July 6, 2001); *see generally* HHS, *Standards for Privacy of Individually Identifiable Health Information* <http://www.hhs.gov/ocr/hipaa/finalmaster.html> (July 6, 2001) [hereinafter HIPAA Guidance]. The HIPAA Guidance refers to the regulations as the "Privacy Rule," and for consistency's sake, this article uses the same moniker. *Id.* § General Overview

6. *See generally Health Insurance Portability & Accountability Act of 1996*, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in sections of 18, 26, 29 and 42 of the United States Code).

7. HHS Fact Sheet, *U.S. Dept. of Health and Human Services, Welfare Reform: Implementing the Personal Responsibilty and Work Opportunity Reconciliation Act of 1996* § Making Welfare a Transition to Work, Work Requirements <http://hhs.gov/news/press/2001pres/01fswelreform.html> (accessed Apr. 4, 2002).

8. HHS News, *U.S. Dept. of Health & Human Services, HHS Issues First Guidance on New Patient Privacy Protections* ¶ 6 <http://hhs.gov/news/press/2001pres/20010706a.html> (accessed Apr. 4, 2002).

9. Compliance with the Privacy Rule is not required until February 2003. 45 C.F.R. § 164.534. Shortly before this article was sent to print, HHS announced that is would propose changes to the Privacy Rule. *See generally* HHS News, *HHS Proposes Changes that Protect Privacy, Access to Care: Revisions Would Ensure Federal Privacy Protections While Removing Obstacles to Care* <www.hhs.gov/news/press/2002pres/20020321a.html> (accessed Apr. 7, 2002) [hereinafter HHS News, *HHS Proposes Changes*]. In general, the proposed changes remove some consent requirements, clarify the application of the "minimum necessary" standard as it applies to oral conversations, addresses issues related to parental

tects privacy by regulating the ways in which certain medical information may be used by certain entities.[10] It also gives patients access to certain information contained in their files. The Privacy Rule is important because it bridges the privacy gap between those interests deemed fundamental by the Supreme Court, and private personal information, in this case relating to medical information, that reasonable people would choose to keep out of the public domain.[11]

Part I of this Article will discuss the various concepts of privacy that exist, and how they apply to personal information. Part II will discuss the key provisions of the Privacy Rule;[12] and Part III will discuss the effects of the Privacy Rule on different entities, and the practical impact the Privacy Rule will have on consumers and commerce as a whole.

II. PRIVACY OF PERSONAL INFORMATION

A. FUNDAMENTAL RIGHT TO PRIVACY

"A person's medical profile is an area of privacy infinitely more intimate, more personal in quality and nature than many areas already judicially recognized and protected."[13]

Not all "privacy" is created equal.[14] The highest level of privacy protection, afforded to a relatively narrow conceptualization of privacy, is the constitutional right of privacy for fundamental rights.[15] Only personal rights that are deemed "fundamental" or "implicit in the concept of

---

access of their children's records, and issues related to marketing of patient information. *Standards for Privacy of Individually Identifiable Health Information*, 67 Fed. Reg. 14776 (Mar. 27, 2002).

10. Office for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information* § General Overview ¶ 2, § Frequently asked Questions, ¶¶ 2, 4 <http://hhs.gov/ocr/hipaa/finalmaster.html> (accessed Apr. 4, 2002).

11. *See generally id.*

12. The Privacy Rule as a whole is dense, technical, and complex. While this Article attempts to set out many of the most significant provisions, there is no substitute for reading the Privacy Rule in its entirety.

13. *Board of Med. Quality Assurance v. Gherardini*, 93 Cal. App. 3d 669, 678 (Cal. App. 1979).

14. One of the earliest articulations of a right to privacy embedded in the law came from Brandeis and Warren in 1890. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). Long before there were concerns about the health care industry violating privacy, the primary concern of privacy advocates involved the press. Paul Starr, *Health and the Right to Privacy*, 25 Am. J.L. & Med. 193, 196 (1999). Early conceptualizations of the right to privacy were postulated in, of all places, law review articles. *But see* Richard A. Posner, *The Future of the Student Edited Law Review*, 47 Stan. L. Rev. 1131, 1133 (1995) (stating that the "Golden Age" for student edited law reviews "drew to a gradual close between 1970 and 1990"). Brandeis and Warren articulated the right to privacy as "the right to be let alone." Warren, *supra* n. 14, at 195-96.

15. *Roe v. Wade*, 410 U.S. 113, 152 (1973).

ordered liberty" rise to this level.[16] Hence, any government attempt to infringe on such a privacy right must survive strict scrutiny.[17]

There is a privacy gap between the amount of privacy afforded to rights deemed fundamental by the Supreme Court, and everything else. Although the Court found a fundamental right to privacy embedded in various Constitutional Amendments,[18] this right is severely limited, and poorly defined.[19] Furthermore, there is no "general interest in freedom from disclosure of private information."[20] To date, the fundamental

16. *Roe*, 410 U.S. at 152; *see U.S. West, Inc., v. FCC*, 182 F.3d 1224, 1236 n. 6 (10th Cir. 1999).

17. *Seal v. Morgan*, 229 F.3d 567, 574-75 (6th Cir. 2000).

> Government actions that burden the exercise of those fundamental rights or liberty interests are subject to strict scrutiny, and will be upheld only when they are narrowly tailored to a compelling governmental interest. The list of fundamental rights and liberty interests—which includes the rights to marry, to have children, to direct the education and upbringing of one's children, to marital privacy, to use contraception, to bodily integrity, to terminate one's pregnancy, and possibly the right to refuse unwanted lifesaving medical treatment, however, is short, and the Supreme Court has expressed very little interest in expanding it.

Id. (citation omitted).

18. *See Griswold v. Conn.*, 381 U.S. 479, 484-85 (1965).

> [Prior] cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'

Id. (citations omitted).

19. Bruce L. Watson, *Disclosure of Computerized Health Care Information: Provider Privacy Rights Under Supply Side Competition*, 7 Am. J.L. & Med. 265, 269 (1981); *see Johnson v. Phelan*, 69 F.3d 144, 154 (7th Cir. 1995). Judge Posner stated that:

> the term 'right of privacy' bears meanings in law that are remote from its primary ordinary-language meaning . . . . One thing it means in law is the right to reproductive autonomy; another is a congeries of tort rights . . . ; still another is the right to maintain the confidentiality of certain documents and conversations. Another and overlapping meaning is the set of interests protected by the Fourth Amendment, which prohibits unreasonable searches and seizures.

Id.

20. *Whalen*, 429 U.S. at 609 (Stewart, J., concurring). The *Whalen* court upheld a New York statute that required the state to track the identities of people that were prescribed certain drugs that, although legal, had a high potential for abuse, such as "opium and opium derivatives, cocaine, methadone, amphetamines, and methaqualone. These drugs have accepted uses in the amelioration of pain and in the treatment of epilepsy, narcolepsy, hyperkinesia, schizo-affective disorders, and migraine headaches." *Id.* at 593 n. 8 (citations omitted); *but see Johnson*, 69 F.3d at 154 (stating that *Whalen* "can be read to imply that

right to privacy has been applied in cases involving "personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education."[21] Therefore, to frame the issue of disclosure or use of medical information as a violation of the fundamental right to privacy is inaccurate.[22]

It is important to realize from the outset that that there have been no fundamental changes in the law that have led to less privacy for an individual's medical information.[23] Instead, the decrease in privacy and confidentiality has come from a variety of factors.[24] While technological advances have given the health care industry the ability to do more with an individual's medical information,[25] computers are not the sole culprit.[26] Many of the stories of the most blatant violations of an individual's privacy are traced to the conduct of another person, or human error.[27] Additionally, the health care industry as a whole has grown and changed, so that many of the participants—ranging from device and

---

the disclosure by or under the compulsion of the government of a person's medical records might invade a constitutional right of privacy, presumably a 'substantive due process' right").

21. *Planned Parenthood v. Casey*, 505 U.S. 833, 851 (1992).

22. The text of the Privacy Rule is preceded by a Preamble that runs for 336 pages in the Federal Register. 65 Fed. Reg. at 82462-798. The Preamble states that "[p]rivacy is a fundamental right." 65 Fed. Reg. at 82464.

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. An anti-abortion group posted on the Internet the medical records of a woman brought to a hospital due to complications from an abortion. AP High Tech News, *Judge Keeps Women's Records Off Net* ¶ 4 <http://compuserve.thirdage.com/news/ap/tech/20010822.3b847de3.2a84.2.html> (Aug. 23, 2001). The woman was also photographed by group members as she was being brought into the emergency room. *Id.* at ¶ 3. The woman has sued members of the group and the hospital for invasion of privacy, and a court entered a preliminary order to have the group cease publication of the woman's records. *Id.* at ¶¶ 5-6. The Preamble to the Privacy Rule provides the following examples of privacy violations:

> A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet.
>
> A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store.
>
> An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS.
>
> The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut.
>
> A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees.
>
> A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy database included names, addresses, social security numbers, and a list of all the medicines the customers had purchased.

pharmaceutical makers to insurers and employers—have an economic interest in obtaining data about individuals that use their products or are affected by a medical condition.[28]

B. Privacy Protections at the State Level

Because there is no fundamental right to privacy in information about ones self, such information can best be protected if viewed as "property."[29] However, granting and strengthening property rights in personal information is a concept that has been slow to be accepted.[30] While there does currently exist certain property, and hence ownership, rights to certain kinds of information, such as trade secret status for some confidential information,[31] much of the personal information about one's self is not protected.[32] Additionally, United States' law is built on the foundational concept that the public is benefited by having access to information.[33] This value creates a tension between the goals of allowing access to information while at the same time protecting the pri-

---

A speculator bid $4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients.

In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women.

A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol.

65 Fed. Reg. at 82467 (citations omitted). Reports of similar disclosures continue to appear regularly in the media. The Washington Post reported that drug maker Eli Lilly accidentally released the e-mail addresses of approximately 600 people who requested an e-mail reminding them to, among other things, to take their dosage of Prozac. Robert O'Harrow Jr., *Prozac Maker Reveals Patient E-Mail Addresses*, Wash. Post E01 ¶ 2 (July 4, 2001) (available at <http://www.washingtonpost.com/wp-dyn/articles/A16718-2001Jul4.html>). In an incident that did not involve medical information, personal information, such as addresses, social security numbers, and student loan amounts received from the state were available on the Georgia Student Finance Commission Web site after the site's firewalls were disabled during routine software installation. Peralte C. Paul, *Privacy Info Exposed on Net: HOPE Scholars' Personal Data Discovered in Routine Search*, Atlanta J. & Constitution 1A ¶ 3 (July 25, 2001).

28. *See* Starr, *supra* n. 14, at 196 (stressing that, in laying blame for decreasing privacy, technological factors must be considered in conjunction with human and economic factors, and that while technology is a factor, computers may be the solution rather than the villain of the problem).

29. Heiser@sims, Papers: Information Privacy § European & American Approaches to Privacy Protection <http:www.sims berkely.edu/wheiser/heiser_privacy.htm> (accessed Apr. 3, 2002).

30. *See generally id.*

31. *See generally Ruckelshaus v. Monsanto*, 467 U.S. 986 (1984).

32. Heiser@sims, *supra* n. 29, at ¶¶ 7, 8.

33. *See generally The Freedom of Information Act*, 5 U.S.C. § 552 (1996).

vacy of individuals.[34]

The idea of placing information in the public domain is found in the Constitution,[35] in what is sometimes called the "intellectual property clause."[36] The intent of the Framers in creating certain monopoly rights for patent and copyright holders was to bring the information contained in the creations into the public domain, primarily to advance the interests of society as a whole.[37]

Strengthening property rights in information allows an individual to better protect himself against some of the drawbacks that technological advancements have brought.[38] Currently, unwanted disclosure of private information is generally treated at the state level.[39] Most states recognize a group of tort actions that allow for redress when privacy is invaded.[40] These torts, generically referred to as "invasion of privacy,"[41] are recognized in the majority of jurisdictions.[42] They are: (1) "appropriation of another's name or likeness";[43] (2) "unreasonable intrusion upon

34. *See e.g.* Amy Harmon, *As Public Records Go Online, Some Say They're Too Public*, N.Y. Times A1 (Aug. 23, 2001).

35. "The Congress shall have the power . . . to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. Const. art. I, § 8(8).

36. *See* Yochai Benkler, *Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information*, 15 Berkeley Tech. L.J. 535, 536 (2000); Mark A. Lemley, *The Constitutionalization of Technology Law*, 15 Berkeley Tech. L.J. 529, 531 (2000).

37. For example, by requiring the patent holder to disclose a written description of the invention that would allow a "person skilled in the art to which it pertains" to make the invention, others are encouraged to improve the invention, and learn the methods from which it was made. 35 U.S.C. § 112 (1994). A secondary reason is to allow the inventor to profit from the work. *See Graham v. John Deere Co.*, 383 U.S. 1, 9 (1966) (discussing the development of patent law and legislation).

38. For example, scanning and imaging technology combined with the access to information on the Internet has led to increases in identify theft. *See generally* Jeff Sovern, *Opting In, Opting Out, or No Options At All: The Fight For Control of Personal Information*, 74 Wash. L. Rev. 1033 (1999) (discussing the multitude of personal information about an individual that is commercially and publicly available, and how access to that information makes it possible to impersonate another in order to obtain identification, credit cards, and other valuable effects).

39. *The First Amendment Handbook, Chapter 2: Invasion of Privacy* ¶ 1 <http://www.rcfp.org/handbook/ view page.cgi?0201> (accessed Apr. 3, 2002).

40. *Id.* at ¶ 3.

41. *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1064 (Colo. App. 1998).

42. The *Restatement (Second) of Torts* recognizes an action for invasion of privacy that would apply to medical records:

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

Restatement (Second) of Torts § 652D (1977).

43. *Restatement (Second) of Torts* § 652A (1977).

the seclusion of another['s] [privacy]";[44] (3) "publicity that unreasonably places the other in [a] false light";[45] and (4) "unreasonable publicity given to the other's private life."[46] Although the first of the four, appropriation of another's name or likeness, is not relevant to disclosure of medical information,[47] depending on the particular facts, one or more of the other three may be crafted into an action for invasion of privacy for unauthorized disclosure of medical information.[48]

The tort of intrusion into the seclusion of another has been previously used is such circumstances. For example, in *Doe v. High-Tech Institute, Inc.*, plaintiff sued defendant for, *inter alia*, invasion of privacy, premised on a theory of intrusion upon seclusion.[49] Plaintiff, a student in a medical assistant training program, disclosed to his professor that he was HIV positive, and requested that the professor not disclose the information.[50] Soon after, the entire class submitted a blood sample for a rubella test.[51] Plaintiff submitted his sample, and signed a consent, with the understanding that the blood would only be tested for rubella.[52] However, the professor requested the laboratory test defendant's sample, but no other samples, for HIV.[53] The result was positive, and the laboratory, pursuant to statute, reported the results to the state Department of Health, as well as to the training program in which defendant was enrolled.[54] The report included plaintiff's name and address.[55] Defendant argued that any privacy interest that plaintiff held in his blood terminated when plaintiff gave up the sample for testing.[56] However, in holding that plaintiff had a cause of action for intrusion upon seclusion, the court of appeals concluded that "a person has a privacy interest in his or her blood sample and in the medical information that may be obtained from it . . . [and that] an additional, unauthorized test, such as alleged

---

44. *Id.*

45. *Id.*

46. *Id.*

47. Natl. Info. Infrastructure Taskforce, *Options for Promoting Privacy on the National Information Infrastructure* § Medical Record Privacy (Apr. 1997) (available at <http://iitf.doc.gov/ipc/privacy.htm>).

48. *Id.*

49. 972 P.2d at 1064. A jury found for plaintiff on his claim of unreasonable disclosure of private facts. *Id.* The trial court dismissed the intrusion upon seclusion claim. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*; *see* Colo. Rev. Stat. § 25-4-1402 (2001).

56. *High-Tech*, 972 P.2d at 1068. The lower court agreed with defendant's arguments that "a person's privacy interest ends once the blood is removed from the body and that, therefore . . . plaintiff had no reasonable expectation of privacy in his blood sample once it was drawn." *Id.*

here, can be sufficient to state a claim for relief for intrusion upon seclusion."[57]

While the federal government has been slow to grant broad privacy protections in medical information about one's self, some states have been quite active in experimenting with ways to protect their citizens.[58] Such experimentation is encouraged by the federal government, and particularly the Supreme Court, as the Court has "frequently recognized that individual States have broad latitude in experimenting with possible solutions to problems of vital local concern."[59]

The state most in-line with HIPAA and the Privacy Rule is Texas. In June 2001, a law that incorporates much of the federal privacy requirements—and goes beyond it in some areas—was enacted.[60] The Texas law has a broader scope and more restrictions on uses of information for marketing purposes.[61] Texas is one of only a few states that has a comprehensive medical privacy statute.[62] Other states generally address privacy in a variety of different places, including a physician's ethical duties[63] and state licensing laws.

Prior to the enactment of HIPAA, other states provided different

---

57. *Id.*

58. *See generally* Health Privacy Project, *The State of Health Privacy: An Uneven Terrain* <http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat_show.htm?doc_id=35309> (accessed Jan. 20, 2002) [hereinafter *The State of Health Privacy*].

59. *Whalen*, 429 U.S. at 597. The Court went on to quote at length the "classic statement" of Justice Brandeis:

> To stay experimentation in things social and economic is a grave responsibility. Denial of the right to experiment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country. This Court has the power to prevent an experiment. We may strike down the statute which embodies it on the ground that, in our opinion, the measure is arbitrary, capricious or unreasonable. We have power to do this, because the due process clause has been held by the Court applicable to matters of substantive law as well as to matters of procedure. But in the exercise of this high power, we must be ever on our guard, lest we erect our prejudices into legal principles. If we would guide by the light of reason, we must let our minds be bold.

Id. (quoting *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (footnote omitted)).

60. Tex. Sen. 11, 77th Leg. (June 17, 2001) (available at <www.adminlaw.org/legislat.htm>).

61. *See generally* Health Privacy Project, *New Medical Privacy Law in Texas* <http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=71582> (accessed Jan. 20, 2002).

62. *See The State of Health Privacy*, *supra* n. 58, at 9. Rhode Island and Wisconsin also have comprehensive privacy legislation. *Id.*

63. "The patient-physician privilege creates a zone of privacy whose purposes are (1) to preclude humiliation of the patient that might follow disclosure of his ailments and (2) to encourage the patient's full disclosure to the physician of all information necessary for effective diagnosis and treatment of the patient." *Gherardini*, 93 Cal. App. 3d at 678-79 (citations omitted).

protections for medical information.[64] California grants perhaps the strongest protections to medical information, in part through a state constitutional amendment that provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[65] This amendment has been repeatedly applied to protect medical records.[66] Colorado has a theft of medical records statute that criminalizes knowingly obtaining a medical record or medical information for a person's own use or the use of another.[67] Similarly, Georgia specifically criminalizes using a computer or computer network with the intention of examining, among other things, a person's medical data.[68]

III. PROVISIONS OF THE PRIVACY RULE

The state of a person's gastro-intestinal tract is as much entitled to privacy from unauthorized public or bureaucratic snooping as is that person's bank account, the contents of his library or his membership in the NAACP."[69]

A. THE NEED FOR THE PRIVACY RULE

By some estimates, over four hundred people are likely to see part or all of a patient's medical record during the typical hospital stay.[70] This has led some members of the health care industry to state that medical record privacy is not just failing, it is "non-existent."[71] When a patient is admitted into a hospital, information is gathered and disseminated to a seemingly endless array of entities.[72] Upon admission, patient information is sent to various departments, 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,

64. *See infra* nn. 56-58 and accompanying text.

65. Cal. Const. art. I, § 1.

66. *Gherardini*, 93 Cal. App. 3d at 678.

67. Colo. Rev. Stat. § 18-4-412 (2001). Colorado has taken the unusual step of creating a property right of an individual in his or her own genetic information. *See* Colo. Rev. Stat § 10-3-1104.7(1)(a) (2001).

68. Ga. Code. Ann. § 16-9-93 (2001).

69. *Gherardini*, 93 Cal. App. 3d at 679.

70. *See* Charity Scott, *Is Too Much Privacy Bad For Your Health?: An Introduction to the Law, Ethics, and HIPAA Rule On Medical Privacy*, 17 Ga. St. U. L. Rev. 481, 483 (2000).

71. *Id.* at 481.

72. *See id.*; *see generally* Am. Health Info. Mgt. Assn., *Flow of Patient Health Information Inside and Outside the Healthcare Industry* <http://www.ahima.org/inforcenter/current/flow_patient.html> (accessed Jan. 20, 2002).

employers.[73] While not every entity will see every record in every case, the potential for information to be seen by many removed from the care of the patient is great.[74] While the Privacy Rule is in no way intended to keep important information out of the hands of those who make decisions affecting patient care, the Privacy Rule will help keep information that identifies who the patient is from those who do not need it, and is intended to keep the amount of information disclosed to the minimum necessary to accomplish the task.[75]

B. Information Governed by the Privacy Rule

The Privacy Rule is intended to protect certain kinds of medical information, and to give a patient certain rights to access and modify medical information in a physician's records.[76] The Privacy Rule by no means applies to every interaction between a patient and physician, nor every document sent to a third party.[77] The Privacy Rule considers various levels of information. In the broad terms, the Privacy Rule defines what is "health information,"[78] and from that, the Privacy Rule governs the subset of "protected health information." Protected health information is health information which is: (1) individually identifiable;[79] and either (2) transmitted electronically, maintained in electronic media;[80] or trans-

73. Scott, *supra* n. 70, at 484-85 (citing Am. Health Info. Mgt. Assn., *Flow of Patient Health Information Inside & Outside the Healthcare Industry* <http://www.ahima.org/inforcenter/current/flow_patient.html>).

74. *See id.* at 488 (citing Woodward, *Sounding Board: The Computer-Based Patient Record and Confidentiality,* 333 New Eng. J. Med. 1419, 1420).

75. Office of Civil Rights, *Standards for Privacy of Individually Identifiable Health Information* § Minimun Necessary, General Requirement, ¶ 1 <http://hhs.gov/ocr/hipaa/finalmaster.html> (accessed Apr. 4, 2002).

76. 45 C.F.R. § 160.103.

77. *Id.*

78. *Id.* Health information is any information that relates to: an individuals past, present, or future condition; the provision of health care to an individual; or an individual's payment related to past, present, or future health care. *Id.*

79. Individually identifiable information is an important concept under the Regulations. It is "health information" that is created or received by a covered entity or employer; and either identifies an individual, or creates a "reasonable bases to believe the information [could] be used to identify [an] individual." *Id.* § 164.501.

80. Electronic media is defined as follows:

> Electronic media means the mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

Id. § 162.103 (2002). The definition of "electronic media" is found in a separate set of regulations also authorized by HIPAA that pertain solely to standards for electronic transactions. *Health Insurance Reform: Standards for Electronic Transactions*, 65 Fed. Reg. 50312 (Aug. 17, 2000) (codified at 45 C.F.R. pts. 160, 162). These regulations are commonly referred to as the "Security Regulations." *Id.* The security regulations adopt "standards for

mitted or maintained in any other form or medium.[81] This last element is a substantial change from the draft version of the Privacy Rule.[82] The draft regulations[83] did not apply to information stored solely in paper format.[84] Instead, the draft regulations applied to information contained in the record itself. So, for example, if information in a paper record (not covered by the draft regulations) was transmitted electronically, by virtue of the transmission, it would then have been covered under the draft regulations. The Privacy Rule as adopted, however, does away with this distinction, and applies to any individually identifiable information, even if it is stored solely on paper and has never been electronically stored or transmitted.[85]

C. Covered Entities And Use Of Protected Health Information

The Privacy Rule applies directly to three "covered entities": health plans, health care clearinghouses, and health care providers.[86] The Privacy Rule also applies indirectly to a "business associate" of a covered entity.[87] A covered entity is prohibited from using or disclosing "protected health information," except as explicitly allowed.[88] An allowable use or disclosure is to the individual;[89] or to carry out treatment, payment, or health care operations—provided the patient has consented and no exceptions apply.[90] This consent provisions has been the object of significant attention, because opponents of the Privacy Rule claim that it would cause the health care industry to grind to a halt. However, the Privacy Rule has several exceptions to the consent requirement that reduce its potential burden to health care providers.[91]

---

eight electronic transactions and for code sets to be used in those transactions." *Health Insurance Reform: Standards for Electronic Transactions*, 65 Fed. Reg. 50312 (Aug. 17, 2000) (codified at 45 C.F.R. pts. 160, 162). In other words, the security regulations seek to eliminate the estimated 400 different formats of electronic data interchange currently being used in the United States for electronic health claims, and replace each type of transaction with a single, universal format. *Id.*

81. 45 C.F.R. § 164.501.

82. *Standards for Privacy of Individually Identifiable Health Information*, 64 Fed. Reg. 59918 (Nov. 3, 1999).

83. *Id.*

84. *Id.*

85. 45 C.F.R. § 160.103.

86. *Id.* § 160.102.

87. *Id.* § 164.502(e)(1)(i).

88. *Id.*

89. *Id.* § 164.502(a)(1)(i).

90. *Id.* § 164.502(a)(1)(iii).

91. *See generally id.* § 164.506(a)(2)(3)(4).

1. *Consent Required for Use or Disclosure*

"[F]undamental to the privacy of medical information is the ability to control [its] circulation!!!!"[92]

Generally, a health care provider will be required to obtain a signed consent from a patient before using or disclosing protected health information for treatment, payment, or health care operations if the provider has an "indirect treatment relationship with the individual."[93] An indirect treatment relationship is one where the treatment is based on the orders of another health care provider, such as what often is the role of a radiologist or pathologist. If there is a direct relationship, and the individual refuses to consent to the disclosure of protected health information for treatment, payment, or operations purposes, the provider may refuse to provide treatment.[94] Additionally, no consent is required before use or disclosure for treatment, payment, or health care operations functions if the patient is in an emergency situation, provided consent is sought as soon as reasonably practicable;[95] if the provider is required by law to provide treatment, and attempts to obtain consent;[96] or if "substantial barriers to communication" prevent a provider from obtaining consent, provided that, in the exercise of professional judgment, such consent can be "clearly inferred from the circumstances."[97] If consent is not obtained for any of the above reasons, the provider must "document its attempt to obtain consent and the reason why consent was not obtained."[98] Generally, consent given to a covered entity cannot be used by another covered entity,[99] unless the entity participates in an organized health care arrangement,[100] in which case a joint consent may be used that conforms with the notice requirements in the Privacy Rule.[101]

2. *Authorization Required for Use or Disclosure*

As stated above, patient consent is generally required before using or disclosing protected health information for treatment, payment, or operations purposes.[102] For other purposes, or as explicitly required, the

92. *Gherardini*, 93 Cal. App. 3d at 678 (exclamations in original).

93. 45 C.F.R. § 164.506(a)(2)(i). An exception to the consent provision also exists if the health care is being provided to an inmate. *Id.* § 164.506(a)(2)(ii).

94. HIPAA Guidance, *supra* n. 5, § 164.506.

95. 45 C.F.R. § 164.506(a)(3)(i)(A).

96. *Id.* § 164.506(a)(3)(i)(B).

97. *Id.* § 164.506(a)(3)(i)(C).

98. *Id.* § 164.506(a)(3)(ii).

99. *Id.* § 164.506(a)(4).

100. *Id.* § 164.506(f)(1).

101. *Id.* § 164.520 (containing the notice requirements).

102. *Id.* § 164.506(a)(1).

covered entity must obtain an authorization.[103] The Privacy Rule contains provisions specifically concerning a use or disclosure of psychotherapy notes,[104] and research information learned through treatment.[105] Other purposes for which an authorization may be required include, for example, marketing, fundraising, employment determinations, and pre-enrollment underwriting.[106] A valid authorization must include, among other things, a "specific and meaningful" description of the information to be used or disclosed;[107] identification of the person or group to whom the information will be disclosed;[108] the date upon which the authorization will expire;[109] and information concerning the individual's right to revoke the authorization, including how to make a revocation, and exceptions to the right to revoke.[110]

3. *Opportunity to Agree or Object to Use or Disclosure*

Under certain circumstances, a covered entity may use or disclose protected health information without a consent or authorization if the individual is informed of the use or disclosure, and has the opportunity to prohibit or restrict the use or disclosure.[111] Unless an objection is made, a provider may maintain a directory of individuals in a hospital,[112] which may be disclosed to "members of the clergy"[113] or someone who asks for the individual by name.[114] An opportunity to object to being included in the directory must be provided.[115] If a provider is unable

103. *Id.* § 164.502(a)(1)(iv).

104. *Id.* § 164.508(a)(2). An exception exists if the use or disclosure is for treatment, payment, or operations purposes and the consent requirements discussed in *supra* notes 93-1001 are met. *Id.* § 164.508(a)(2)(i). Additionally, no authorization is required for use by the originator of the notes for treatment; or use or disclosure by the covered entity for training purposes or to defend a legal action brought by the individual. *Id.* § 164.508(a)(2)(i)(A)-(C).

105. *Id.* § 164.508(f). For the requirements and exceptions for an authorization in these circumstances; *see* 45 C.F.R. § 164.508(f)(1)-(2).

106. 65 Fed. Reg. at 82463.

107. 45 C.F.R. § 164.508(c)(6)(c)(i).

108. *Id.* § 164.508(c)(6)(c)(iii).

109. *Id.* § 164.508(c)(6)(c)(iv).

110. *Id.* § 164.508(c).

111. *Id.* § 164.510. A covered entities' request to use or disclose, and an individuals agreement or objection, may be oral. *Id.*

112. *Id.* § 164.510(a). The directory may include the individual's name; location in the facility, condition described in "general terms;" and religious affiliation. *Id.* § 164.510(a)(i).

113. *Id.* § 164.510(a)(1)(ii)(A). The purpose behind this provision is to allow the continued practice of clergy members announcing to their congregations that a fellow member of the congregation or the community is ill. *Id.* Some critics of HIPAA have alleged, incorrectly, that HIPAA prevents this activity. *See generally id.*

114. *Id.* § 164.510(a)(1)(ii)(B). In this circumstance, religious affiliation may not be disclosed. *Id.*

115. *Id.* § 164.510(a)(2).

to give the individual the opportunity to object because of the person's condition, the information may still be used if such use is consistent with a previous preference and, in the "professional judgment" of the provider, is in the "best interest" of the individual.[116] A covered entity may disclose protected health information to family and friends of a patient that is "directly relevant to such person's involvement with the individual's care or payment related to the individual's health care" unless the person objects.[117] If the person is unable to express approval or disapproval, the entity may make disclosures based on its "reasonable inferences" of what's in the patient's best interest.[118]

D. Rights of Access by Individuals

Covered entities are required to disclose to an individual protected health information upon that person's request.[119] The Privacy Rule creates a right of access, inspection, and to receive protected health information held by a covered entity, unless the information is psychotherapy notes, or compiled for use in a legal proceeding.[120]

Certain denials by a covered entity of a request to access information are final, and may not be reviewed.[121] Examples of non-reviewable denials are if the covered entity is a correctional facility and allowing access would potentially harm or threaten someone, or if the information was obtained in the course of research.[122] Some denials are reviewable.[123] If a denial is because a licensed health care professional has determined that allowing access will "endanger the life or physical safety of the individual or another person," including a person referenced in the information,[124] the individual may request that the "reviewing official" of the covered entity re-evaluate the denial.[125] Within thirty days of receiving a request,[126] the covered entity must either produce the requested information[127] or issue a written denial.[128] If the entity does not have the

116. *Id.* § 154.510(a)(3).
117. *Id.* § 154.510(b)(1).
118. *Id.* § 154.510(b)(3).
119. *Id.* § 164.502(a)(2)(i).
120. *Id.* § 164.524(a)(1)(i)–(ii).
121. *Id.* § 164.524(a)(2).
122. *Id.* Additionally, denials required by the *Privacy Act*, 5 U.S.C. 552(a) (2001), and denials caused by necessity of keeping a source confidential, are not reviewable. *Id.*
123. *Id.* § 164.524(a)(3).
124. *Id.*
125. A covered entity must appoint a licensed health care professional, who has not participated in the original decision to deny, as a reviewing official. *Id.* § 164.524(a)(4).
126. *Id.* § 164.524(b)(1).
127. *Id.* § 164.524(b)(2)(i)(A).
128. *Id.* § 164.524(b)(1)(i)(B). If the request is denied, the entity must still provide information contained in the request to which the denial does not apply. The denial must

information, but knows where it is maintained, it must so direct the requestor.[129] When providing information to the individual, the covered entity must make it available in the form requested.[130] If the information is not available in that form, a hard copy may suffice.[131]

E. Disclosure Limited to the "Minimum Necessary" Amount of Information

One of the most significant privacy safeguards implemented by the Privacy Rule is the "minimum necessary" standard.[132] The standard applies anytime a covered entity uses or discloses protected health information itself, or requests protected health information from another covered entity.[133] In either event, "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."[134] There are various common sense exceptions to the standard, such as information coming from or going to a health care provider for treatment purposes.[135] This insures, contrary to what various critics argued, that treatment will not suffer as a result of a physician having an incomplete grasp of a patient's condition.[136] The Privacy Rule does not specify exactly how an organization must implement the necessary protocols, only that policies and procedures should reflect the "business practices and workforce" of the entity.[137] The HIPAA Guidance makes clear that case-by-case review is not necessary for routine disclosures, but that when a procedure allows a group access to a patient's entire medical file, such

---

state the reason for the denial and, if applicable, a description of the procedure the individual may follow in order to complain. *Id.* § 164.524(d)(2).

129. *Id.* § 164.524(d)(3).

130. *Id.* § 164.524(c)(2)(i).

131. *Id.* § 164.524(c)(2)(i).

132. *Id.* § 164.502(c).

133. *Id.* § 164.502(b)(2).

134. *Id.* § 164.502(b)(2) (emphasis added). *See infra* nn. 141-144 and accompanying text (providing a discussion of the effects of the "reasonable efforts" qualifier to the minimum necessary standard).

135. 45 C.F.R. § 164.502(b)(2)(i). Additionally, the minimum necessary standard generally does not apply to uses or disclosures made to the individual, the Secretary of Health and Human Services, or uses or disclosures required by either the law or for compliance with the Regulations, such as an audit. *Id.* § 164.502(b)(2)(ii)-(iv).

136. The HIPAA Guidance discusses attempts by the Secretary to clarify the application of the minimum necessary standard in treatment settings, and states that HHS will propose changes to the Privacy Rule to "increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high quality health care. We understand that issues of this importance need to be addressed directly and clearly to eliminate any ambiguities." HIPAA Guidance, *supra* n. 5, § Minimum Necessary.

137. *Id.*

allowance must be explicit, and include a justification.[138]

1. *Development of Reasonable Criteria for Non-Routine Disclosures*

Non-routine disclosures of personal health information are treated differently under the minimum necessary standard.[139] For these cases, a covered entity must develop "reasonable criteria" that will function to limit the amount of personal health information disclosed.[140] These non-routine disclosures must be reviewed on case-by-case basis, with decisions made based on reasonable criteria.[141] The development of reasonable criteria for non-routine disclosures applies to the party requesting the personal health information as well as to the party potentially disclosing it.[142] The party that is requested to disclose personal health information, may, under certain circumstances, defer to the judgment of the party making the request, if the request is "reasonable under the particular circumstances of the request."[143]

2. *Using Reasonable Efforts to Limit Disclosure of Personal Health Information*

Compliance with the minimum necessary standard will vary from one entity to another.[144] This is because the Privacy Rule only requires "reasonable efforts" to comply with the standard.[145] In other words, what is reasonable will vary between a large hospital with a electronic record system and a solo practitioner with a paper-based system. The HIPAA Guidance states that "facility redesigns" would not generally be required to meet the reasonableness standard.[146] In other words, controlling access to information in a paper-based system would, at the least, require keeping patient files in locked cabinets that could be accessed only by certain individuals. Entities that already use electronic systems would at a minimum need passwords on machines containing personal information.[147] The HIPAA Guidance also addresses two widely held misunderstandings of the minimum necessary standard as it applies to x-rays and sign-in sheets.[148] Under the Privacy Rule, x-ray

138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.* Reasonable reliance is permitted when the request is made by: another covered entity; under circumstances for which a consent or authorization is not required; or by an employee or business associate of the covered entity holding the information. *Id.*
144. *Id.*
145. *Id.* § 164.502(b)(1).
146. *Id.* §§ 164.502(b), 164.514(d).
147. *Id.* § 164.502(b).
148. HIPPA Guidance, *supra* n. 5, § Minimum Necessary.

boards do not have to be totally isolated from the public—a covered entity must merely take reasonable precautions to protect personal health information displayed on them.[149] Additionally, the common use of sign-in sheets is not affected, and HHS intends to propose modifications to the Privacy Rule clarifying its intent to not alter practices related to either.[150]

F. Business Associates

While the Privacy Rule will have a direct impact on the covered entities—providers, clearinghouses, and health plans—business associates of covered entities are also affected. A "business associate" assists a covered entity in a function involving the use or disclosure of protected health information.[151] A covered entity can also be a business associate of a covered entity based on the services it supplies.[152] A covered entity may disclose protected health information to a business associate, and allow a business associate to create or receive protected health information on behalf of the covered entity, if the covered entity obtains "satisfactory assurances" that the business associate will appropriately safeguard the information.[153] These safeguards must be documented in a contract or other written agreement between the covered entity and the business associate.[154] The contract must: establish the permitted and required uses and disclosures of information; and limit the activities of the business partner to those that could be undertaken by the covered entity.[155] The Rules set out the steps a covered entity must take if it knows that a business partner is breaching its obligation under the contract.[156] In the case of a breach, the covered entity must: take reasonable steps to end the violation or breach, terminate the contract if the breach or violation is not remedied, or report the problem to the Secretary of HHS if termination is not feasible.[157]

G. Required Policies and Procedures

An area of the Privacy Rule's greatest impact will be on the organizational changes that covered entities will be required to implement. For example, a covered entity must designate a privacy official who is

149. *Id.*

150. *Id.*

151. 45 C.F.R. § 160.103. Examples of such functions include billing, claims processing or administration, data analysis, and utilization review. *Id.*

152. *Id.* Examples of services rendered that could make the provider a business associate include legal, accounting, consulting, administrative, accreditation, and financial. *Id.*

153. *Id.* § 164.502(e)(1).

154. *Id.* § 164.502(e)(2).

155. *Id.* § 164.504(e)(2)(i).

156. *Id.* § 164.504 (e)(1)(i).

157. *Id.* § 164.504(e)(2).

"responsible for the development and implementation of the policies and procedures of the entity,"[158] and a person responsible for receiving complaints.[159] All employees must be trained about the entities policies and procedures about protected health information.[160] Reasonable safeguards are required to protect against inadvertent disclosure.[161] Additionally, a covered entity must keep records of all its policies and procedures, and must keep records of any complaints it received concerning its policies and procedures.[162]

IV. PREDICTED EFFECTS OF THE PRIVACY RULE

While the full ramifications of the Privacy Rule will not be known until some time after compliance becomes mandatory, based on its requirements, covered entities will be forced to make certain changes in their policies and procedures regarding protected health information that should have definite effects which are clearly evident to patients. Still other effects will be internal in nature, and not apparent to those outside of the covered entity. Finally, various aspects of compliance will surely require assistance from companies outside of the health care industry. For example, it is likely that consultants and attorneys will be hired to help covered entities, especially large hospitals or insurance companies who have the potential for the greatest liability should they fail to comply with the Privacy Rule, to draft and implement the various policies and procedures, and the appointment of personnel to serve in the positions described in the Privacy Rule. Finally, because the Privacy Rule was designed with medical information in electronic form in mind, it is likely that covered entities will rely on software developers to design programs with automated features to comply with the minimum necessary standard, as well as security standards.

A. COVERED ENTITIES

While there was a general consensus from the health care community that patient privacy could be improved, the ways by which the improvements were to be accomplished brought bitter disagreement. HHS recognized the far-reaching and fundamental changes that the Privacy Rule implementation will bring.[163] Therefore, substantial lead time for covered entities to prepare for implementation exists.[164] In the end,

158. *Id.* § 164.530(a)(1)(i).
159. *Id.* § 164.530(a)(1)(ii).
160. *Id.* § 164.530(b)(1).
161. *Id.* § 164.530(c)(1).
162. *Id.* § 164.530(d)(1).
163. HHS News, *HHS Proposes Changes*, *supra* n. 9, at ¶ 1.
164. *Id.* at ¶ 12.

many of the provisions of the Privacy Rule reflect compromises between privacy advocates and industry leaders.[165] It seems likely that additional changes in the Privacy Rule will reflect remaining concerns from those in the health care industry.

Many of the Privacy Rule's requirements will be felt mostly by the covered entities, rather than patients. Those provisions that have the greatest potential to alter the health care landscape have been discussed within.[166] These provisions fall into two general categories, those that require a covered entity to adopt certain internal procedures,[167] and those that require new procedures directed at patients.[168] Examples of the former include adopting "minimum necessary" disclosure procedures.[169] Examples of the latter will require covered entities to obtain, in certain circumstances, a consent or authorization from a patient before using or disclosing personally identifiable health information.[170]

One of the Privacy Rule's greatest impacts will likely be felt on a group to which the privacy rule does not even apply directly. Because business associates must adequately safeguard information obtained from covered entities, many of the same provisions will apply to, for example, auditors or attorneys that work for covered entities.[171] For instance, a law firm that represents a hospital in a malpractice case will need to provide virtually the same protections when handling medical files as the hospital.

B. PATIENTS

Some of the Privacy Rule's effects on patients can be stated with certainty, while others are merely hopeful. For example, it is a certainty that, with some exceptions, patients will have newfound control over information contained in their medical records.[172] This applies to who has access to the information, as well as the patient's own access to the information.[173] Although many States currently have legislation pertaining to the circumstances under which a health care provider must provide a patient with information contained in his records,[174] the Privacy Rule

165. *Id.* at ¶¶ 14-16.

166. *See* 45 C.F.R. §§ 160-64.

167. 45 C.F.R. §§ 164.514(a), 160.103, 164.501, 164.502(e), 164.516(e), 164.501, 164.508(f), 164.512(f), 160.300, 164.512(c), 164.512 (f).

168. *Id.* §§ 166.502(8), 164.506, 164.502(c).

169. *Id.* §§ 166.502(c), 164.514(d).

170. *Id.* §§ 164.506, 164.502(c).

171. *Id.* §§ 160.103, 164.502(e), 164.516(e).

172. *Id.* §§ 166.502(c), 164.514(d).

173. *Id.*

174. *Id.*

provides a nationwide uniform standard.[175] Patients, however, should not presume that obtaining the full array of protections and rights under the Privacy Rule will be easy to acquire.[176] On the contrary, patients will have to be on guard against inadvertently authorizing a use or disclosure of personal medical information that is unintentional.[177]

The hopeful effect of the Privacy Rule is that information in a person's medical records will be seen by fewer people,[178] thus lessening the chance for intrusion into a person's private and confidential life. As a result, the opportunity for improper use of the information is lessened. Such uses, ranging from publication to advance a personal or political agenda, to marketing to accomplish financial goals, have occurred repeatedly in the past.

C. COMMERCE

A significant amount of medical information gathered by providers, insurers, and clearinghouses is already in electronic form.[179] Part of the challenge under the Privacy Rule will be how to develop software that can efficiently, yet accurately, apply the Privacy Rule's requirements.[180] For example, it is foreseeable that a covered entity would want to develop software that would give different levels of access to information depending on the access level defined in a password. So, for example, while a doctor or nurse would have access to an entire file, a receptionist might have access to only a patient's name, address, and phone number—and not the results of medical tests—while a claims processor might have access to an amount of information somewhere in between.

V. CONCLUSION

While the Supreme Court has recognized a fundamental right to privacy in some circumstances, this right is limited, and not likely to expand.[181] Furthermore, although the Court has also recognized the inherent potential for abuse when large amounts of personal information is gathered in computer databases, the Court has not been willing to expand the fundamental right of privacy to personal information about one's self.[182] The Privacy Rule should go a long way in closing a gap between protections given to fundamental privacy rights, and all other privacy rights.

---

175. *Id.*
176. *Id.* § 164.508.
177. *Id.*
178. *See generally* HHS News, *HHS Proposes Changes*, *supra* n. 9.
179. 45 C.F.R. §§ 160, 164.
180. *Id.*
181. *See generally Roe*, 410 U.S. 113.
182. *Id.*