Georgia State University Law Review

Volume 17
Issue 2 *Winter 2000*

Article 1

12-1-2000

Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy

Charity Scott

IS TOO MUCH PRIVACY BAD FOR YOUR HEALTH? AN INTRODUCTION TO THE LAW, ETHICS, AND HIPAA RULE ON MEDICAL PRIVACY*

Charity Scott†

INTRODUCTION

> "I can tell you unequivocally that patient confidentiality is not eroding—it can't erode, because it's simply nonexistent."—Mark Hudson, former health insurance company employee.[1]

After years of debate, Congress has still not enacted comprehensive laws to protect the privacy of medical records. Defaulting on its own self-imposed deadline of August 1999 to enact such legislation, Congress tossed this political hot potato to the Department of Health and Human Services (HHS). In December 2000, HHS Secretary Donna Shalala issued nearly 400 pages of privacy regulations, the first 340 pages of which are preamble and comments to explain the complex new federal rule. State laws on medical privacy are so abstruse and

---

* This article originally appeared as *Is Too Much Privacy Bad For Your Health? An Introduction to the Law and Ethics of Medical Privacy, in* PRIVACY AND HEALTH CARE 1 (James M. Humber & Robert F. Almeder eds., 2001), and is reprinted, with updating revisions, with permission of the publisher. The original version of this article was written just after the Department of Health and Human Services (HHS) issued proposed regulations on the privacy of health care information in November 1999. *See* Standards for Privacy of Individually Identifiable Health Information, Proposed Rule, 64 Fed. Reg. 59918 (Nov. 3, 1999). These proposed regulations were promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 2021 (1996). As this current revision was being prepared for publication, HHS issued final regulations on health care privacy. *See* Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164, as corrected by Technical Corrections to Final Rule, 65 Fed. Reg. 82944 (Dec. 29, 2000)). The current article has been updated to incorporate the final HIPAA rule on health care privacy. Both the proposed rule and the final rule are available at http://aspe.hhs.gov/admnsimp/index.htm.

† Professor of Law, Georgia State University College of Law.

1. *See* Maggie Scarf, *Keeping Secrets*, N.Y. TIMES, June 16, 1996, § 6, at 38.

intricate—so "extensive, vast, and detailed"[2]—that words commonly used to describe them include "patchwork," "erratic," and "morass."[3]

Why is it so hard to enact simple, straightforward laws to protect the privacy of medical records? Nearly everyone agrees that it is ethically right to ensure the confidentiality of patients' health information. Just how much privacy protection to give that information, however, is a question over which people sharply disagree. Patients often believe that no one except their closest health caregivers should be able to see their medical records without their prior permission. Many others, mostly strangers to the patient, believe they should be allowed to look at those records without first having to ask the patient's permission. These strangers justify having relatively free access to medical information on the ground that it is good for the patient, good for other patients, or good for society at large. Perhaps not coincidentally, such access may also be good for the people accessing the records.

This Article examines why the ethical and legal debates over medical privacy have proven so intractable for so long. It organizes the competing interests and values in the debates by exploring two questions. First, how much privacy *do* we actually now have? Surprisingly little. Part I identifies who currently has relatively free access to our medical records and discusses many authorized and unauthorized uses of the information in those records. Second, how much privacy *should* we have? This question is addressed from both ethical and legal perspectives. Medical ethics has long championed the privacy of individual patients, but in the name of general societal welfare, we have long tolerated considerable sacrifices in personal privacy. In effect, we have assumed that too much privacy could be bad for your—or at least, for our collective—health. Part II analyzes the ethical trade-offs that we have made between the benefits of ensuring patient privacy on one hand, and the societal goods we have derived from sacrificing it on the other hand (such as

2. JOY PRITTS ET AL., HEALTH PRIVACY PROJECT, INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY, THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN: A COMPREHENSIVE SURVEY OF STATE HEALTH PRIVACY STATUTES (Executive Summary) (1999), *available at* http://www.healthprivacy.org/usr_doc/35309.pdf.

3. *See* Andrew A. Skolnick, *Opposition to Law Officers Having Unfettered Access to Medical Records*, 279 JAMA 257, 257 (1998).

advances in scientific research, protection of the public health, higher efficiency and better quality in the delivery of health care, and even improved law enforcement). Finally, Part III explores how the laws to date have reflected this ethical balancing. A potential third question—how much privacy *can* we have in light of current computer technology and security devices—is reserved for another day.

I. HOW MUCH PRIVACY DO WE HAVE?

> "Privacy has disappeared—get used to it."—Lawrence O. Gostin, health law and policy expert.[4]
>
> "There is a long gravy train forming around our medical records."—Charles Welch, M.D., chairman of the Massachusetts Medical Society's task force on confidentiality policy.[5]

The Institute of Medicine suggests that an "exhaustive list" of patient record users would parallel the list of everyone associated, directly or indirectly, with the provision of health care, including at a minimum sixty-seven categories of representative individual and institutional users (and multiple individuals within each category may actually have access to the record information).[6] The Congressional Research Service reported that an estimated 400 people may see at least some portion of a patient's medical record during the course of a single hospital stay.[7]

A. Authorized Access to Patient Health Information

Take the typical hospital record: the information contained in it may be disclosed widely both inside and outside of the

---

4. Arthur Allen, *Exposed: Computer Technology, Managed Health Care and Genetic Science Are All Undermining the American Tradition of Medical Privacy, in the Name of Progress: What Can or Should We Do About It?*, WASH. POST MAG., Feb. 8, 1998, at W10.

5. Maggie Scarf, *Brave New World: The Threat to Privacy That Didn't Go Away*, THE NEW REPUBLIC, July 12, 1999, at 16.

6. *See* COMMITTEE ON IMPROVING THE PATIENT RECORD, INSTITUTE OF MEDICINE, THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE (Richard S. Dick et al. eds., rev. ed., Nat'l Acad. Press 1997).

7. *See* Sue Blevins, *Medical Privacy Invasion?*, WASH. TIMES, July 22, 1999, at A17.

hospital.[8] The primary uses of this information are for direct patient care and for billing and payment.[9] In connection with patient care, many health care professionals (such as physicians, nurses, specialists, allied health personnel, and residents and students in a teaching hospital) need the patient's record to provide appropriate medical treatment and nursing care.[10] Many others have access to the record to provide related diagnostic or ancillary services (such as radiology or pathology departments, laboratories, physical and respiratory therapy, dietary services, social services, and discharge planning).[11] In connection with payment, many users both inside the provider's facility (for example, the billing and accounts offices) and outside the facility (for example, third-party payers such as health plans, insurers, managed-care organizations, employers, government agencies, and the clearinghouses that transmit the claims information) review patient records to determine whether and how much to pay for health care services under a staggering variety of benefits plans and programs.[12]

Secondary users of patient health information include those who work in numerous supporting services that are important for the efficient and effective functioning of the health care system (such as quality assurance and risk management, medical education, peer review of individual professionals, accreditation of the facility, and biomedical research).[13] Tertiary users include people or organizations offering private or for-profit services (such as third-party benefits managers, marketers, and database developers).[14] They also include government agencies that collect and use health information to perform their functions, such as public health authorities (for example, many states mandate the reporting of infectious diseases, child or elder abuse, domestic violence, gunshot

8. A graphic chart of where patient information flows both inside and outside the health care industry is available at the American Health Information Management Association's Web site and forms the basis for this discussion. *See* AHIMA, *Flow of Patient Health Information Inside and Outside the Healthcare Industry*, *at* http://ahima.org/media/flow_patient.html (last visited Jan. 11, 2001).

9. *See id.*

10. *See id.*

11. *See id.*

12. *See id.*

13. *See id.*

14. *See id.*

wounds, or abortions), bureaus of vital statistics and immunization registries, immigration services, and social welfare services.[15] In addition, schools may require medical information (for example, information related to allergies, medications, and sports fitness); such information may end up in the courts (for example, litigation involving malpractice, personal injury, or even divorce, adoption, and child custody matters); and police and other law enforcement officers may seek patient records in order to investigate crimes against individual persons (for example, rape, assault, drug use, or drunk driving) and against the government (for example, under the health care fraud and abuse laws).[16]

Finally, medical information is finding its way onto the Internet. Hospitals are experimenting with putting patient records on the Internet not only to improve the quality and efficiency of health care services (for example, to allow clinical information to be quickly accessed in an emergency room across town) but also to empower patients to read their own records and even to challenge the information contained in them.[17] Doctors are going on the Web to communicate with patients through e-mail and to take advantage of Web-based services.[18] Patients themselves are voluntarily putting their health information online—from prescription medications to living wills to electrocardiograms—at such sites as drkoop.com or PersonalMD.com as an aid to their families and doctors in case of emergency, as well as to learn more about health topics pertinent to their own situations.[19]

Unfortunately, even with clearly stated privacy policies, health Web sites often fail to protect consumer privacy. A recent report investigating twenty-one health Web sites found an inconsistency between the sites' actual privacy practices and

---

15. *See id.*
16. *See id.*
17. *See* Greg Borzo, *PCASSO with a Mouse*, AM. MED. NEWS (LOG ON), Oct. 13, 1997, *available at* http://www.ama-assn.org/sci-pubs/amnews/net_97/logo1013.htm.
18. *See* Mike Mitka, *Weaving Webs for Physicians*, 281 JAMA 1070, 1070-71 (1999); *see also* Ron Winslow, *The Doctor: As Medical Sites Proliferate on the Web, More Physicians Are Shedding Their Technophobic Past*, WALL ST. J., Dec. 8, 1997, at R10.
19. *See* Ann Carrns, *Patients' Next Choice: Whether To Keep Files Stored on the Internet*, WALL ST. J., Aug. 16, 1999, at B1.

their stated privacy policies.[20] Moreover, the study found that "[e]ven with the best intentions, many sites do not have adequate security in place to protect consumer information from the casual hacker or someone actively seeking to access company databases."[21] With this introduction, we now turn to the subject of unauthorized users and uses of medical information.

B. Unauthorized Invasions of Patient Privacy

Although most people are unaware just how routinely and extensively their medical information is disseminated throughout the health care system, most of the above uses of medical records are authorized or permitted under current law. It is the occasional well-publicized horror story of abusive or unauthorized access to patient information that prompts sporadic outcries to "do something" to protect the privacy of medical records. People become most concerned that information about themselves will not be kept confidential when such information is the kind that can be used against them—information that can harm their economic, social, or emotional well-being.

Disclosure of sensitive medical information—for example, HIV infection, sexually transmitted disease, genetic predispositions, or mental illness—can cause embarrassment, acute distress, or social stigmatization. Patients' fears of losing the respect and goodwill of others is just one dimension to their fear of losing their privacy. Fear of losing their jobs or insurance or otherwise suffering discrimination in the marketplace also creates motivation to ensure that their medical facts are kept secret. Indeed, some reports indicate that people were denied or lost their jobs or insurance coverage when information about their genetic risks was disclosed.[22] Fears of job-related or other economic discrimination are not unfounded, in light of a 1996

---

20. JANLORI GOLDMAN ET AL., CALIFORNIA HEALTHCARE FOUNDATION, PRIVACY: REPORT ON THE PRIVACY POLICIES AND PRACTICES OF HEALTH WEB SITES (2000), *available at* http://admin.chcf.org/documents/ehealth/privacywebreport.pdf.

21. *Id.* at 4.

22. *See* David L. Coleman, *Who's Guarding Medical Privacy?*, 17 BUS. & HEALTH 3, 20 (1999); *see also* B.P. Fuller et al., *Privacy in Genetics Research*, SCIENCE, Aug. 27, 1999, at 1359-61.

survey reporting that one-third of Fortune 500 employers admitted using their employees' medical records in making employment decisions.[23] In one well-known account, a banker allegedly was able to use computerized medical records to determine which of his customers had cancer, and he called in their loans early.[24]

Some of the anecdotes recount goofs, or accidental disclosures of medical records. For example, while the University of Michigan's health system was trying to resolve problems with its new patient scheduling system, it put thousands of patient records on the Internet instead of on what it thought was a secure system.[25] Two months passed before a medical student discovered the mistake.[26] When the Harvard Community Health Plan computerized the medical records of its 300,000 subscribers, it inadvertently gave many of its employees full access to the detailed psychotherapy notes about patients.[27]

Other stories reflect intentional, even malicious, invasions of privacy. In Massachusetts, a convicted child rapist got a job in a hospital, and by using someone else's password, he was able to access almost 1000 computerized patient records, which he used to make obscene phone calls to young girls.[28] In Maryland, clerks obtained patient information from the state's Medicaid database and sold the data to four HMOs.[29] In Florida, a public health worker took a computer disk with 4000 names of HIV-positive patients and sent it to two newspapers.[30]

Celebrities and political candidates are at high risk for widespread publication of their health information. A hospital worker leaked to a newspaper the fact that the late tennis

---

23. *See* THE CENTER FOR PUBLIC INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY 27 (1998), *available at* http://www.publicintegrity.org/nothing_sacred.pdf [hereinafter NOTHING SACRED]; *see also* Coleman, *supra* note 22.

24. *See* Beverly Woodward, *Sounding Board: The Computer-Based Patient Record and Confidentiality*, 333 NEW ENG. J. MED. 1419, 1421 (1995).

25. *See* Jodi Upton, *U-M Medical Records End Up on Web*, DETROIT NEWS, Feb. 12, 1999, at A1.

26. *See id.*

27. *See* Alison Bass, *HMO Puts Confidential Records Online*, BOSTON GLOBE, Mar. 7, 1995, at 1; *Privacy? At Most HMOs You Don't Have Any*, USA TODAY, July 13, 1998, at A12.

28. *See* John Riley, *Case Study: With Old Password, Cracking the Code*, NEWSDAY, Mar. 31, 1996, at A30.

29. *See* Woodward, *supra* note 24, at 1420.

30. *See* Coleman, *supra* note 22.

champion Arthur Ashe was infected with HIV.[31] Although country singer Tammy Wynette had tried to protect her privacy by entering a hospital under a pseudonym, a hospital employee apparently accessed her records and revealed them to the National Enquirer.[32] During Nydia Velazquez's campaign for election to the House of Representatives, she learned that information about her previous suicide attempt and subsequent mental health care had been anonymously faxed to the New York media and given widespread publicity.[33] Although ultimately elected, she found the disclosures acutely embarrassing professionally and personally—she had not even told her parents.[34]

One of the most pervasive abuses of medical records privacy is also often viewed as one of the most innocent: the perennial "browsing" by a health care organization's employees of the medical records in the system's computers. An employee's ability to access the records easily through a password is often simply assumed to grant permission to do so. Health care workers may view patient records "for such diverse reasons as curiosity (e.g., about friends, neighbors, relatives, or celebrities), perversity (e.g., sexual interests), anger (e.g., on the part of an employee who is about to be or has recently been dismissed), or a desire for financial or political gain."[35] Although common, such browsing by insiders is usually an abuse of medical records access privileges. Sometimes employees may be disciplined for such unauthorized access, but more often their viewing of patient records is not detected nor even considered wrong.[36]

C. The Example of Managed-Care Oversight: Legitimate Disclosures or Unethical Invasions of Privacy?

Distinguishing an abuse of medical privacy from a legitimate need to see a patient's records is often a difficult question. What patients and their doctors may view as intolerable snooping by

31. *See* NOTHING SACRED, *supra* note 23, at 27.
32. *See* John Riley, *Open Secrets: Changes in Technology, Health Insurance Making Privacy a Thing of the Past*, NEWSDAY, Mar. 31, 1996, at A5.
33. *See* Scarf, *supra* note 5.
34. *See id.*
35. Woodward, *supra* note 24, at 1420.
36. *See* Coleman, *supra* note 22.

health plan representatives may be defended by those health plans as necessary oversight to ensure both high-quality and cost-effective health care. Mental health records provide a good example.

Managed care organizations (MCOs) often want extensive information about a patient-subscriber's condition before they will pay for extensive therapy sessions or expensive medications.[37] Representatives of MCOs or the prescription drug benefit companies that have been hired by the MCOs routinely contact psychiatrists to review their patients' records. To get authorization for therapy or for medications, psychiatrists complain they have to give highly detailed information about the patient's problems, her symptoms, estimates as to how long therapy is expected to last, justifications for prescribing one drug over a cheaper alternative, and so on.[38] According to a Baltimore psychiatrist, "[T]he more specific you are, the more dirty laundry you give them, the more approvals you get."[39] A clinical social worker flatly stated: "These days, you can't just put down the diagnosis—say, 'depression.' No, you have to get very specific, to state that this woman is depressed because she's involved in a masochistic, self-destructive affair with her boss, or that this man has gotten depressed around a sexual dysfunction and hasn't been able to respond to his partner for the past few years."[40]

The MCOs defend the practice as necessary to ensure quality of care at a reasonable cost for their subscribers' mental health treatment.[41] The observations of the CEO of a large California mental health management organization are typical. He explains that MCOs are responding to prior histories of "people getting into outpatient therapy and literally spending years there, with no treatment goals and no concern about the resources being expended for the treatment," and he argues that "the increased demand for detailed personal information is part and parcel of what first brought managed-care organizations into being—the need for a sense of discipline and

37. *See* Allen, *supra* note 4; Scarf, *supra* note 1.
38. *See* Allen, *supra* note 4; Scarf, *supra* note 1.
39. Allen, *supra* note 4.
40. Scarf, *supra* note 1.
41. *See id.*

accountability, which was totally lacking in the mental health care field."[42] Some physicians also defend the practice of giving MCOs patients' information as an aid to improving patient care. One doctor, who switched drugs for several patients after discussing their care and alternatives with a company representative, stated: "I didn't see anything that was ethically wrong with that . . . If the insurance company is paying for medication, that insurance company has a right to know."[43]

Although subscribers usually signed a blanket authorization form for access to medical records when they joined the health plan, psychiatrists acknowledge that patients often are completely unaware of exactly what those forms mean. The tension between loyalty to the unsuspecting patients to keep their most intimate and personal revelations confidential and the psychotherapist's practical desire to get paid for treating them can be quite stark. "I have children to put through college,"[44] said one psychiatrist who permitted a records audit without telling his patients. "When I retire, maybe I'll be more brave."[45] Psychiatrists say they now give the equivalent of a *Miranda* warning to their patients: "Be careful! Anything you say can and will be widely shared and held against you by your insurance company."[46] The American Psychiatric Association estimates that forty percent of patients now pay out of their own pockets to avoid these disclosures of their mental health information.[47]

In light of many people's extensive and easy access to a patient's health information—some with clearly legitimate interests, some with clearly illegitimate ones, and many falling in the large, murky middle—we might understandably ask whether "medical privacy" has become an oxymoron.

---

42. *Id.*

43. Robert O'Harrow Jr., *Between Doctor and Patient, a Three-Way Relationship: Adding a Pharmacy Benefit Manager to Treatment Mix Can Bring Interference, Information, and Savings*, WASH. POST, Sept. 27, 1998, at A26.

44. Allen, *supra* note 4, at 151.

45. *Id.*

46. A.G. Breitenstein, *Let States Fill the Gap*, USA TODAY, Apr. 6, 1998, at 11A.

47. *See Privacy? At Most HMOs You Don't Have Any*, *supra* note 27.

II. HOW MUCH PRIVACY SHOULD WE HAVE?

> "All that may come to my knowledge in the exercise of my profession . . . which ought not to be spread abroad, I will keep secret and will never reveal."—Hippocratic Oath[48]

Americans feel a strong sense of entitlement to health care privacy, even though most are unaware how often and to whom their health information is routinely disclosed. Consumer polls over the past decade have overwhelmingly shown that Americans highly value privacy and believe laws should protect it. According to one 1999 survey, ninety percent of Americans think that health insurance companies sharing medical records with other companies is an invasion of privacy.[49] Another 1999 poll reported that eighty-five percent of Americans support new federal laws to protect medical privacy.[50] In a 1998 poll, ninety percent of consumers said it was either "extremely important" or "very important" to them personally in choosing a health plan to have confidence that the health plan and providers would keep their records completely confidential.[51] A 1996 Time/CNN poll reported that eighty-seven percent of Americans think laws should be passed to prohibit health care organizations from giving out medical information without first getting the patient's permission.[52] According to an oft-cited 1993 Louis Harris poll, eighty-five percent of respondents said protecting the confidentiality of medical records was "absolutely essential" or "very important," and ninety-six percent thought

---

48. Skolnick, *supra* note 3, at 257.

49. *See* Peter D. Hart Research Associates, Shell Poll (released May 1999), *available at* Westlaw, POLL Database, QUESTION ID: USHART.SH99MR R23B5, no. 088. Sixty-seven percent of respondents considered sharing of medical records a "major" invasion of privacy; twenty-seven percent called it a "minor" invasion. *See id.*

50. *See* Press Release, California HealthCare Foundation, Americans Worry About the Privacy of Their Computerized Medical Records (Jan. 28, 1999), *available at* http://www.chcf.org/press/view.cfm?itemID=362.

51. *See* National Partnership for Women & Families, Family Matters Survey (released Feb. 1998), *available at* Westlaw, POLL Database, QUESTION ID: USLAKESP.98FAMILY R85, no. 082. Sixty-one percent responded that medical records confidentiality was "extremely important," and twenty-nine percent responded that it was "very important." *See id.*

52. *See* Yankelovich Partners, Inc., Time/CNN/Yankelovich Partners Poll (released Feb. 1996), *available at* Westlaw, POLL Database, QUESTION ID: USYANKP.022396 R29, no. 043.

it was important that all personal medical information be designated as sensitive, that penalties be imposed for unauthorized disclosures, and that laws spell out who has access to medical records and what information could be obtained.[53]

A. Ethical Underpinnings of a Right to Medical Privacy

Why do we feel so strongly entitled to a right to medical privacy? Going all the way back to the Hippocratic Oath quoted earlier, there are certainly long-standing ethical foundations for such a right. As a philosophical matter, respect for privacy reflects respect for autonomy and for an individual's desires to develop her own sense of self and to shape the relationships she has with others.[54] Just ask any teenager how important privacy is for the development of identity and personal growth. As a practical matter, respect for privacy may be justified in light of the harms that can result from disclosures of personal information. A court recently characterized unauthorized disclosures of patient information as invading two distinct interests: "(1) the patient's interest in the security of the confidential relationship and his corresponding expectation of secrecy; and (2) the patient's specific interest in avoiding whatever injuries will result from circulation of the information."[55]

Depending on to whom the disclosures are made (for example, to a spouse, a friend, an employer), the harms that result from invading this second patient interest could include severe emotional, social, or economic injury—embarrassment, humiliation, social stigma, marital discord, loss of reputation, and even loss of a job or insurance. If these potential harms are

---

53. *See* Louis Harris & Associates, Equifax-Harris Poll (released Nov. 1993), *available at* Westlaw, POLL Database, QUESTION ID: USHARRIS.110593 R3C, nos. 008, 010, 015; *see also* Wirthlin Group (released June 1994), *available at* Westlaw, POLL Database, QUESTION ID: USWIRTH.94JUNE R10H, no. 011 (reporting that most people said they were either "extremely concerned" (55% of respondents) or "somewhat concerned" (27%) about the privacy of their medical records); Electronic Privacy Info. Ctr., Medical Privacy Opinion Polls, *at* http://www.epic.org/privacy/medical/polls.html.

54. *See* Lawrence Gostin, *Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations*, 127 ANNALS OF INTERNAL MED. 683 (1997), *available at* http://www.acponline.org/journals/annals/supplement/protect.htm.

55. Biddle v. Warren General Hospital, No. 96-T-5582, 1998 WL 156997, at *3 (Ohio Ct. App. 1998) (citing Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1434 (1982)), *aff'd*, 715 N.E.2d 518 (Ohio 1999).

perceived as sufficiently great, the patient may decide to withhold health-related information from her doctor in the future, thus suffering harm to the first patient interest as well, namely, impairment in the doctor-patient relationship itself. Indeed, the harms from actual or feared disclosures can be so devastating that many patients take extraordinary steps in their dealings with health care professionals to ensure that their health information is kept secret. In a recent study, one in six Americans reportedly engages in such "privacy-protecting behaviors" as switching doctors; paying for health care out-of-pocket; asking a doctor to not write down certain information in their record or to record a less serious or embarrassing health condition; giving inaccurate information in their medical history; or even not seeking medical care in the first place for a health problem.[56] These "privacy-protecting behaviors" or "defensive measures" raise obvious health risks, threaten the integrity of the doctor-patient relationship, and could skew medical research based on patient records.[57]

That many Americans feel their medical privacy is jeopardized reflects their ethical intuitions that they are entitled to have their medical information kept private in the first place. These intuitions are in turn supported by the professional ethics codes that govern health care professions and professional associations. The professional codes of nearly every health care profession (for example, the ethics codes for physicians, nurses, dentists and dental hygienists, mental health professionals, social workers, pharmacists, and chiropractors) and the ethical standards of numerous health care professional associations (for example, hospitals and health care executives) all explicitly require respect for the principles of privacy and confidentiality.[58] The codes may refer to privacy or confidentiality as a "core value" or a "fundamental tenet" and

---

56. *See* California Health Care Foundation (press release), *supra* note 50; *see also* Amy Goldstein, *Long Reach Into Patients' Privacy: New Uses of Data Illustrate Potential Benefits, Hazards*, WASH. POST, Aug. 23, 1999, at A1.

57. *See* Woodward, *supra* note 24, at 1421; *see also* Janlori Goldman, *Protecting Privacy to Improve Health Care*, 17 HEALTH AFFAIRS 47 (1998).

58. *See generally* CODES OF PROFESSIONAL RESPONSIBILITY: ETHICS STANDARDS IN BUSINESS, HEALTH, AND LAW (Rena A. Gorlin ed., BNA 4th ed. 1999) (compiling ethical codes and standards for health care professions).

usually make respect for privacy a central or guiding principle of the health professions.[59]

If there is so much general agreement among patients and their health care professionals upon the principle that patients are entitled medical privacy, then what is the problem with simply drafting our laws to reflect that societal consensus? While privacy may be valued in principle, it is not considered an absolute ethical right. Like all ethical values, it is often balanced against competing ethical values and concerns. The American Medical Association's (AMA) Code of Medical Ethics is a typical example of this qualification on the privacy right. The AMA Code begins with a clear affirmation of the privacy right and a strong prohibition against disclosures: "The patient has a right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient...."[60] However, the Code moderates this language with a qualification on the privacy principle: "UNLESS provided for by law or by the need to protect the welfare of the individual or the public interest."[61] This exception—allowing disclosures for the benefit of the patient or the public—has proven so enormous that some would argue it has swallowed the rule.

The benefits of disclosure to the patient and to the public can be great, as discussed in more detail later. Often, the benefits of disclosures are not readily apparent until after prohibitions against disclosures are strictly enforced. One recent example from Maine illustrates these benefits of disclosure, as well as the proposition that it is possible to have "too much" privacy.[62] In January 1999, the Maine legislature enacted a tough new law prohibiting the release of a patient's medical information without her written permission.[63] This simple and direct prohibition was backed up with heavy fines for violation.[64] The impact was swift and dramatic: hospitals refused to give any information over the telephone to family and friends inquiring

59. *See generally id.*

60. American Med. Ass'n, Code of Medical Ethics, Fundamental Elements of the Patient-Physician Relationship, Element No. 4, reprinted in CODES OF PROFESSIONAL RESPONSIBILITY, *supra* note 58, at 342.

61. *Id.*

62. *See* Goldstein, *supra* note 56.

63. *See id.*

64. *See id.* The potential fine was up to $50,000 per patient. *See id.*

about a patient's status; florists said they could not deliver flowers; priests said they could not see patients for last rites; newspapers said they would be hindered in reporting on accident victims.[65] Even doctors could not compare notes on the same patient without getting written permission from the patient, and clinical labs refused to give patients their results over the telephone.[66] The law was repealed within two weeks and replaced with a less restrictive version, and one of its original drafters commented, "What we really did . . . [is] protect patients more than they wanted to be protected."[67] Maine citizens seem to have concluded that too much privacy could be bad for their health.

B. The Benefits of Privacy Versus the Benefits of Disclosure: Where Should We Strike the Ethical Balance?

How much privacy is *too much* privacy? When should the principle of privacy give way to obtain the benefits of disclosure—both in the patient's interest and for the public's welfare? As the Maine experience illustrates, strict privacy protection laws have their costs. Our society has always thought it was worth making trade-offs between protecting patient privacy and promoting both the patient's and the public's health. This section describes some of the social goods—benefits to the community as a whole—for which we have traditionally sacrificed individual privacy. Within each category of social benefit, this section also raises an example to illustrate how difficult it often is to resolve, ethically and legally, whether a similar trade-off should continue to be made in the future.

1. Safeguarding the Public's Health

We have tolerated substantial losses of a patient's privacy when the patient posed a serious health risk to others. We have allowed, or even required through public health laws, doctors to disclose to family members or to public agencies when a patient

---

65. *See id.*

66. *See* Thomas Lee, *Too Much Privacy Is a Health Hazard*, NEWSWEEK, Aug. 16, 1999, at 71.

67. Goldstein, *supra* note 56 (quoting Gordon H. Smith, an official of the Maine Medical Association).

has an infectious disease that poses a high risk of contagion.[68] For example, public health laws aimed at monitoring or controlling the spread of communicable diseases address the reporting of such illnesses as sexually transmitted diseases, HIV and/or AIDS infection, hepatitis, and tuberculosis. Public health monitoring of patterns of violence has also justified requiring physicians (and others) to report evidence of gunshot wounds, domestic violence, and child abuse.[69] In some cases, psychiatrists have been held to a legal duty to reveal their patient's confidences, without their patient's consent, by warning others that their patient has threatened to kill or seriously injure them.[70] All of these disclosures without the patient's consent—or breaches of confidentiality, if you will—have been justified in the name of protecting the public's safety or welfare. Too much patient privacy was thought hazardous to the public's health.

Yet not everyone agrees that public health measures justify sacrificing individual privacy. One current illustration of the ethical tensions between patient privacy and public health involves childhood vaccination registries.[71] In Illinois, for example, registry advocates would like to expand their computerized database to track the vaccination histories of all children.[72] A comprehensive registry makes it easy for any doctor or nurse to check quickly whether a child's vaccinations are up-to-date, which is helpful in a mobile society where families move frequently, and which might be critical in a sudden visit to an emergency room when the parents may not remember exactly what shots were given to their child and when. Families in poorer neighborhoods who may receive less regular and consistent medical care than families in more affluent neighborhoods would especially benefit from such a database. Opponents argue that these health benefits are outweighed by the threats to privacy that vaccine registries

68. *See generally* BARRY R. FURROW ET AL., HEALTH LAW § 4-34, at 151 (1995) (enumerating various mandatory disclosures under state and federal law).

69. *See id.*

70. *See id.*; *see also* Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334 (Cal. 1976).

71. *See* Frank James, *Children's Vaccine Registry Raises Medical Privacy Fears*, CHI. TRIB., May 7, 1999, at 1.

72. *See id.*

pose.[73] Registry critics are concerned that such databases would quickly be expanded beyond childhood vaccinations to the creation of medical files on every American, which ultimately could be used by government, insurers, or others to the detriment of individual citizens.[74]

2. Facilitating Medical Research

We have also tolerated sacrifices in patient privacy in the name of scientific progress. For decades, medical researchers have collected and analyzed a multitude of data culled from the medical records of thousands of patients, often without the patients' knowledge or explicit consent. The researchers have used this information to advance scientific understanding of the causes, treatment, and prevention of diseases. Has the appropriate ethical balance been struck between patient privacy and medical research if scientific researchers may gain access to this information in patients' records without their express prior permission?

Developments in Minnesota present a case in point. Until recently, researchers in Minnesota were not required to obtain patients' express consent before reviewing their medical records in connection with a scientific research project.[75] This relatively unrestricted access for scientific purposes has allowed researchers at, for example, the renowned Mayo Clinic to monitor the outcomes of care and evaluate the effectiveness of new treatments since the early part of this century.[76] This medical records research has been credited with, among other things, helping the Mayo Clinic achieve its reputation for high quality of care and with supporting thousands of studies and publications to advance scientific medical knowledge.[77] Ethically speaking, the clear benefits to scientific progress were evidently thought to outweigh the apparently minimal privacy intrusions into patients' medical records.

---

73. *See id.*
74. *See id.*
75. *See* L. Joseph Melton III, *The Threat to Medical Records Research*, 337 NEW ENG. J. MED. 1466, 1467-69 (1997).
76. *See id.* at 1467.
77. *See id.*

The Minnesota legislature changed the law effective January 1997, and the new law reflects a shift in the ethical balance.[78] The new law requires medical researchers to notify all patients in writing that their records may be used for research and to obtain patient authorization for access to their records.[79] One author explains that by this law, "any potential social benefits of epidemiological research were discounted in favor of privacy."[80]

This shift in the ethical balance brought cries of protests. Health care researchers complained that the new law would require excessive expense and bureaucratic burden to contact all of the hundreds of thousands of patients seen every year and get their written authorization.[81] Moreover, since the vast majority of patients would probably expressly consent in any event, the law would result in needless costs and burdens on the health care system.[82] Critics also charged that the law would distort scientific studies because those patients who refused to consent to giving researchers access to their medical records would be excluded from any study, thus potentially resulting in selection bias.[83] Some of these charges seem to have been borne out in practice. One recent study on the empirical effects of the new Minnesota law found that it resulted in low participation rates and increased time to complete medical research.[84] The study concluded that "[e]fforts to protect patient privacy may come into conflict with the ability to produce timely and valid research to safeguard and improve public health."[85]

Did the Minnesota legislature tip the ethical balance too far in favor of patient privacy? Critics have thought so.[86] Some have

---

78. *See id.*
79. *See id.*
80. *Id.*
81. *See id.*
82. *See id.*
83. *See id.* at 1467-68; *see also* Thomas J. Liesegang, *Potential Effect of Authorization Bias on Medical Record Research*, 128 AM. J. OPHTHALMOLOGY 129 (1999) (describing Mayo Clinic study in which authors concluded that "laws requiring written authorization for research use of medical records could result in substantial biases in etiologic and outcome studies").
84. *See* Douglas B. McCarthy et al., *Medical Records and Privacy: Empirical Effects of Legislation*, 34 HEALTH SERV. RES. 417, 417-25 (1999).
85. *Id.*
86. See Association of Am. Med. Coll., *Confidentiality of Medical Records: AAMC Report on the Minnesota Experience*, Issue Briefs Forum, *available at*

urged that a more appropriate balance is struck under the federal regulations for the protection of human subjects in research, often referred to as the Common Rule.[87] Although these regulations provide that researchers obtain the express, informed consent of human subjects prior to undertaking research on them, they also provide for an exception. An Institutional Review Board (IRB) may waive this informed consent requirement if it finds that the research project poses "no more than minimal risk" of harm to the subjects and that the research could "not practicably be carried out without the waiver" of the consent requirement.[88] As a practical matter, these two conditions allow IRBs often to waive the informed consent requirement in cases involving medical records research.[89] Privacy advocates worry that when IRBs judge a retrospective medical records research project to be socially or scientifically desirable, they are too easily persuaded both that it is "not practicable" to get consent from a large number of patients and that the harm to them from such research is "minimal" as well, with the consequence that a "right to privacy that is easily and frequently overridden on grounds of social utility is no longer a right."[90] There is also considerable recent evidence that the IRBs' protections for patient confidentiality are weak both in principle and in practice.[91]

So where should we strike the ethical balance between patient privacy and the advancement of medical research? The controversy over medical records research has ardent advocates on both sides. The new Minnesota law reflects one balance, and

---

http://www.aamc.org/advocacy/issues/research/minrepot.htm (last visited Sept. 7, 2000) [hereinafter *AAMC Minnesota Report*] (concluding that the "Minnesota statute poses a number of threats to research and may threaten both health policy and public health objectives").

87. *See* Melton, *supra* note 75, at 1469.

88. 45 C.F.R. § 46.116(d) (2000).

89. *See* U.S. GEN. ACCOUNTING OFFICE, MEDICAL RECORDS PRIVACY: ACCESS NEEDED FOR HEALTH RESEARCH, BUT OVERSIGHT OF PRIVACY PROTECTIONS IS LIMITED, GAO/HEHS-99-55, at 14 (1999), *available at* http://www.gao.gov/cgi-bin/getdoc.cgi?dname=gao&docid=f:he99055.txt.pdf [hereinafter GAO Report 99-55].

90. Beverly Woodward, *Medical Record Confidentiality and Data Collection: Current Dilemmas*, 25 J.L. MED. & ETHICS 88, 91 (1997); *see also* Beverly Woodward, *Challenges to Human Subject Protections in US Medical Research*, 282 JAMA 1947, 1947-52 (1999) [hereinafter Woodward, *Challenges*].

91. *See* GAO Report 99-55, *supra* note 89.

the federal Common Rule involving the protection of human research subjects reflects another.

3. Improving Health Care Quality, Access, and Accountability

The above two categories reflected trade-offs between an individual's privacy interests and the larger community's interests in public health and medical research. Much of the current controversy over the limits of medical privacy reflects a tension between privacy protection and efforts to improve quality of care—arguably for the patient's own benefit, or for the benefit of similarly situated patients.

Managed-care health plans and other health insurers, for example, say that their unrestricted access to their subscribers' medical records—usually under a blanket authorization form signed by the subscriber upon enrollment in the plan—is the key to controlling health care costs and improving health care quality.[92] To support their claims that their access to your medical information is good for your health, managed-care organizations point to a variety of programs that they can offer based on your (and other health plan subscribers') medical data. With computers, for example, health plans can compile and analyze large amounts of data to generate statistics, or report cards, on how well they are providing health services, so that consumers may judge the plans' quality and make informed choices about their health. By reviewing patients' medical records, a health plan can also send reminders to its subscribers for mammograms or other routine preventive care, resulting in earlier interventions and ultimately better (and cheaper) care.[93]

Based on patient record review, a health plan also may analyze patterns in certain kinds of care and be able to

---

92. *See* Allen, *supra* note 4; Scarf, *supra* note 1.

93. *See* Karen Ignagni, *Do Not Retard Progress*, USA TODAY, July 13, 1999, at 12A (observing that health progress could not occur without relatively unrestricted information-sharing); Robert Pear, *Future Bleak for Bill To Keep Health Records Confidential*, N.Y. TIMES, June 21, 1999, at A12 (noting that insurers and HMOs routinely use information in patient files to contact them concerning health benefits, "to detect fraud, to learn which treatments are most effective, to evaluate the work of individual doctors and to identify those who order too many tests and procedures," and they argue that "it is totally impractical for them to request permission each time they want to use a patient's medical records").

recommend alternative and improved care. For example, if records show repeated emergency hospital visits by a child with asthma or an adult with diabetes, the plan may be able to intervene and arrange more effective care at an earlier stage than at the emergency room.[94] Many health plans have developed so-called "disease management programs" to encourage subscribers with specific illnesses to take advantage of preventive health care offerings.[95] After reviewing subscribers' medical records, for example, Aetna U.S. Health Care contacts certain subscribers and their doctors, "asking whether patients with diabetes would like a free kit to test their blood-sugar levels at home or whether congestive heart patients would like a home visit from a nurse to help them stick to a salt-free diet and keep tabs on their weight."[96]

Whether such analyses of medical records are justified by improved quality of care or lowered costs, or whether they constitute unwarranted invasions of privacy, is often a judgment call, and people will disagree over whether the call was correctly made. For example, Harvard Pilgrim Health Care in Boston analyzed their subscribers' medical records to determine which ones had made three expensive emergency room visits.[97] The plan learned that many of these subscribers were alcoholics, and the next time they visited an emergency room, their primary care doctors were notified and instructed to talk with the patient.[98] A Harvard Pilgrim official commented, "I don't know how the alcoholics react when their doctor calls and says, 'I hear you were in your third automobile accident.'"[99]

One highly publicized controversy between protecting a patient's privacy and disclosing her medical information ostensibly for her own benefit involves health plans' use of pharmacy benefit managers (PBMs).[100] When a patient fills a prescription at a pharmacy using her health plan's prescription card, her information is entered into a computer that transmits

---

94. *See* Ignagni, *supra* note 93.
95. *See* Goldstein, *supra* note 56.
96. *Id.*
97. *See* Allen, *supra* note 4.
98. *See id.*
99. *Id.*
100. *See* Robert O'Harrow Jr., *Plans' Access to Pharmacy Data Raises Privacy Issue; Benefit Firms Delve into Patient Records*, WASH. POST, Sept. 27, 1998, at A1.

it instantly to the plan's PBM. The PBM checks to see, among other things, if the drug is approved, if there are equally effective and cheaper alternatives, or if the drug is safe for this particular patient. The PBM may respond with alternative suggestions for the patient while she is waiting at the pharmacy counter.[101]

The health plans argue that this disclosure of prescription information is justified in the name of quality care and cost control.[102] They say it allows them to recommend cheaper and often more effective alternative medications for their subscribers, with resulting enormous cost savings annually on prescription drugs.[103] PBM services also provide a system for cross-checking that patients are not taking dangerous drug combinations, especially helpful when a patient may be seeing multiple doctors who are unaware of the others' prescriptions.[104] In some cases, the system can alert patients and their doctors to the risks of taking certain medications too long; in other cases, it can remind patients when they are due for refills for their prescriptions, to aid in ensuring that they are complying with long-term drug regimens.[105]

Privacy advocates, on the other hand, argue that these intrusions into patient privacy do not necessarily improve their health, and they cite accounts in which plans mistakenly made assumptions about their subscribers' health status solely on the basis of their prescription information.[106] For example, one woman whose doctor prescribed her an antidepressant for sleep disorders due to menopause was erroneously encouraged to sign up for the health plan's anti-depression program.[107] Privacy advocates, and even some government regulators, are worried that these PBMs are more concerned with the marketing of, or steering patients to, their parent company's own drugs than

101. *See id.*; *see also* O'Harrow, *supra* note 43.
102. *See* O'Harrow, *supra* note 100.
103. *See id.* (reporting GAO estimate of $600 million in prescription cost savings in the federal employees health program in 1995); O'Harrow, *supra* note 43 (reporting PBM official estimates of $3 billion in annual drug cost savings for health plans nationally).
104. *See* O'Harrow, *supra* note 100.
105. *See id.*
106. *See id.*
107. *See id.*

with the patient's health; three of the top PBMs are owned by Eli Lilly & Co., SmithKline Beecham, and Merck & Co.[103]

Where should we strike the balance in medical privacy? Health plans argue it would utterly defeat their efforts to improve quality and contain costs to insist that they get their subscribers' prior consent for every use of their medical record (hence their resort to the initial blanket authorization form). Others argue that we are getting too close to the wrong side of the ethical line that distinguishes medicine from marketing, and that invasions of privacy are becoming justified less by medical ethics (whose goal is the patient's best interest) than by business ethics (whose goal is to make a profit).[103]

4. Assisting Law Enforcement

We have also allowed intrusions into individuals' medical privacy in the name of public safety. For example, police may put out a description of a fleeing injured suspect and ask that hospitals report any patient who may come to the emergency room matching that description. Federal fraud investigators may comb through hundreds or even thousands of patient records at a hospital to detect patterns of billing fraud in the hospital's claims for Medicare or Medicaid reimbursement. These are viewed as legitimate law enforcement activities. To the extent they are undertaken without the patient's authorization, however, they are invasions of the patient's privacy. Do the social benefits justify such intrusions?

Law enforcement officers argue strenuously that the public's safety and welfare demand that they have relatively unfettered access to patient records.[110] State police officers and district attorneys have cited instances in which quick access to medical information proved critical in apprehending a suspect (for example, the recent case of a convicted arsonist of at least ten

---

108. *See id.*

109. *See* Robert O'Harrow, Jr., *Prescription Sales, Privacy Fears: CVS, Giant Share Customer Records With Drug Marketing Firm*, WASH. POST, Feb. 15, 1998, at A1 (discussing the context of two retail drug stores' disclosure of patient prescription information to a database marketing firm, and quoting medical ethicist Robert Veatch that "the conflict is so basic it's probably indefensible"). *See infra* notes 129-30 and accompanying text.

110. *See* Stuart A. Van Meveren, *Don't Hinder Crime-Fighting*, USA TODAY, Aug. 20, 1999, at 14A.

churches across three states), or in which privacy protections could undermine prompt investigations of child abuse or domestic violence.[111] Federal law enforcers testified to Congress that the price of privacy is too high if it would hinder their efforts to fight fraud in the health care industry.[112] The FBI and Department of Justice are opposed to any new regulation to require them to notify patients in advance that the agencies were going to search the patients' medical records for evidence of provider fraud.[113] These federal agencies are convinced that such a requirement could have a "devastating effect" in their battle against health care fraud and abuse.[114]

Privacy advocates argue that the balance has been tipped too far in favor of law enforcement activities to the detriment of individual privacy and health. They point out that, under current federal law, the records of which videos you rented last weekend are given more protection from police snooping than are your medical records.[115] In their zealous efforts to prosecute health care providers for fraud, law enforcers may be insufficiently attentive to the privacy interests of patients. Last year, for example, the names of 274 patients were matched with their individual laboratory tests on billing statements and were erroneously included as part of the public record in court documents filed by federal prosecutors in Kansas.[116]

Mental health professionals in particular are concerned that their role in healing is being threatened by demands for their cooperation in policing.[117] Trust in the confidential nature of the psychotherapist-patient is of utmost importance to the therapeutic process.[118] If the patient does not believe his

---

111. *See id.*

112. *See* Kristen Hallam, *Price of Privacy May Be Too High: FBI, Justice Department Say Patient Confidentiality Bills Would Threaten Fraud Crackdown*, MODERN HEALTHCARE, May 13, 1999, at 12.

113. *See id.*

114. *See id.*

115. *See* Video Privacy Protection Act, 18 U.S.C. § 2710 (1993) (requiring warrant, grand jury subpoena, or court order).

116. *See* J. Duncan Moore Jr., *Confidentiality Casualty: Patient Billing Printouts Released in Kansas Fraud Case*, MODERN HEALTHCARE, Sept. 14, 1998, at 3; *see also A Trail of Mistakes Led to Breach of Patient-Data Confidentiality*, MODERN HEALTHCARE, Sept. 21, 1998, at 80.

117. *See* Skolnick, *supra* note 3, at 259.

118. *See id.*

confidences will be kept, she is less likely to reveal them. Furthermore, even if revealed, the psychotherapist may be disinclined to write them down out of concern they may be disclosed during investigations. Both reactions can jeopardize the efficacy of the therapeutic relationship and the integrity of the medical record itself.[119]

III. LAW AS A REFLECTION OF ETHICAL BALANCING

As the above four illustrations have shown, society has tolerated significant trade-offs in individual privacy for numerous benefits in public health, safety, and welfare. But sharp disagreements remain over whether many of these trade-offs have been worth it and whether similar trade-offs should be tolerated in the future. These ethical tensions—and our difficulties in agreeing on the right ethical trade-offs—are reflected in the state of our laws, both at the state and federal level. The ethical debates have been aired loudly and repeatedly in Congress in recent years, and many have attempted to forge consensus over a federal privacy law. To date, however, various competing interests and starkly different views over where we should strike the appropriate ethical balance have stymied all efforts to pass such federal legislation. At the state level, each state has enacted its own different set of privacy rules, often resulting in complexity within each state's laws and lack of uniformity across state lines.

A. State Laws on Medical Privacy

According to a recent survey of state laws by Georgetown University's Health Privacy Project, only three states have a single, comprehensive set of laws on health privacy.[120] All of the others have adopted their laws on a piecemeal basis over time, with the result that the laws "can be found in nearly every nook and cranny of a state's statutes—in obvious and obscure sections of a state's code, buried in regulations, developed in case law, and detailed in licensing rules."[121] Georgia, for

119. *See id.*
120. *See* PRITTS ET AL., *supra* note 2 (Executive Summary).
121. *Id.*

example, has about ninety separate statutes addressing some aspect of health care privacy, and that number does not include the case law developed by court decisions or regulations created by state agencies.

Why is there such complexity in state laws on health privacy? In part, this complexity reflects the numerous different users—and uses—of health information. States tend to regulate according to each different entity that may collect, use, or disseminate health information.[122] For example, Georgia has separate laws governing health information in the hands of: physicians, hospitals, schools, HMOs and other health insurers, nursing homes, pharmacies, researchers, and various public agencies (from the state's benefits programs to the state personnel board to others such as the coroner's office, Department of Motor Vehicles, jails and prisons, or workers' compensation board).[123] Like other states, Georgia also tends to regulate by specific disease conditions.[124] There are separate statutes addressing, for example, AIDS and HIV, sexually transmitted diseases, genetic information, mental health illnesses and disabilities (including mental retardation), alcohol and drug abuse and treatment.[125] Additional complexity is layered on by the nature of the rules themselves, with some laws requiring that confidentiality must be kept (for example, for HIV or AIDS infection or information considered privileged by courts) and with others requiring or permitting disclosure of health information to public agencies or to others (as, for example, in cases of child abuse, elder abuse, non-accidental injuries, certain sexually transmitted diseases, vital statistics, spinal cord injuries, and unusual or suspicious deaths).[126]

Also contributing to the piecemeal approach of state laws on health privacy is the fact that usually laws are enacted over time rather than as a collection all at one time. They are often responsive to a particular issue which attracts enough public attention for state legislators to be called on to "do

122. *See id.*
123. *See id.* (Georgia Summary).
124. *See id.*
125. *See id.*
126. *See id.*; *see also* Leonard J. Panzitta & T. Mills Fleming, *Hospital Medical Records*, *in* GEORGIA HOSPITAL LAW MANUAL (4th ed. 1997).

something."[127] Citizens tend to call on government to shift the ethical balance when certain perceived wrongs become highly publicized, and a law is then passed to correct the perceived ethical imbalance. Last year in Georgia, for example, a new health privacy statute was enacted to prohibit health insurers from selling prescription information received from a pharmacy without a patient's written consent.[128] This new law was perhaps responsive to the media uproar caused the year before by reports that certain retail drug stores (including CVS Corp. and Giant Food Inc.) had been selling patients' prescription information to a database marketing specialist, who in turn used that information both to remind patients to get prescription refills and to market other drugs by mailing "educational material" from drug manufacturers to patients with particular illnesses.[129] Georgia's law reflects the state's position on the ethical issues raised by this conduct. Although CVS defended it as "good medical and good entrepreneurial practice," evidently Georgia sided with those who viewed such conduct as a "breach of fundamental medical ethical issues."[130]

B. Current Federal Laws on Medical Privacy Other Than the HIPAA Rule

> "My head hurts from dealing with this issue."—Senate aide complaining after dozens of unsuccessful meetings to negotiate compromise federal legislation.[131]
>
> "This privacy stuff is its own little monster."—Robert Gellman, former congressional staff member and consultant on medical privacy.[132]

---

127. *See* PRITTS ET AL., *supra* note 2 (Executive Summary).
128. *See* O.C.G.A. § 33-24-59.4 (2000).
129. *See* O'Harrow, *supra* note 109; *see also* Robert O'Harrow Jr., *CVS Also Cuts Ties to Marketing Service; Like Giant, Firm Cites Privacy on Prescriptions*, WASH. POST, Feb. 19, 1998, at E1.
130. O'Harrow, *supra* note 109 (quoting George D. Lundberg, then-editor of the Journal of the American Medical Association).
131. Louise D. Palmer, *Privacy Bill For Patients Is Debated*, BOSTON GLOBE, June 7, 1999, at A1.
132. Goldstein, *supra* note 56.

In light of the enormous numbers of differing state laws on health privacy, it is no wonder there have been calls for a single, comprehensive, and uniform set of federal laws to govern health privacy. And yet, in light of the multitude of scenarios in which legitimate claims of patient privacy must be balanced against legitimate claims for access to patient records, Congress has been unable to pass such federal legislation. Although Congress has been hearing testimony about problems in health records confidentiality since 1971,[133] the federal laws addressing health privacy have still been quite limited until now.

The principal federal privacy law, the Privacy Act of 1974, regulates how the federal agencies may collect, use, and disseminate personal information about individuals.[134] The Freedom of Information Act (FOIA) generally allows citizens access to records held by federal agencies, but it contains nine exceptions that permit the agencies to withhold certain information, including personnel and medical files if disclosure would constitute a clearly unwarranted invasion of personal privacy.[135] Several federal agencies, such as the Department of Health and Human Services and the Centers for Disease Control and Prevention, have used these FOIA exceptions to resist disclosure of health data and patient or research records.[136]

A few federal laws address the confidentiality of specific kinds of health records. These laws include the federal regulations concerning the confidentiality of human subject research records (the Common Rule, discussed earlier); Medicare regulations requiring hospitals to ensure the confidentiality of patient records;[137] and regulations governing the confidentiality of records of patients who are treated at federally-funded facilities for alcohol abuse or drug abuse.[138] Also, the Americans With Disabilities Act requires employers to keep employees' medical records confidential.[139] This law has

133. *See* NOTHING SACRED, *supra* note 23, at 5.
134. 5 U.S.C. § 552a (1994).
135. 5 U.S.C. § 552(b)(1)-(9) (1994).
136. *See* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 501-03 (1995).
137. 42 C.F.R. § 482.24(b)(3) (1999).
138. 42 U.S.C. § 290dd-2 (1994); 42 C.F.R. pt. 2 (2000).
139. 42 U.S.C. § 12112(d)(3)-(4) (1994).

been interpreted by several recent courts to require the confidentiality of all employees' (not just disabled employees') medical records.[140]

The United States Supreme Court has suggested, in principle, that individuals have a right to informational privacy under the United States Constitution.[141] Like most federal legislation, however, a constitutional privacy right would protect only against government disclosures of information, not disclosures of health information by the private sector.[142] Moreover, the federal courts balance this individual right against competing state interests in public health, safety, and welfare, often resulting in a judicial balancing which, like the ethical balancing described earlier, may tolerate a wide range of government disclosures of individuals' health information.[143]

C. New HIPAA Rule on Medical Privacy

As part of a health care reform package known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[144] Congress gave itself three years (until August 1999) to enact comprehensive legislation to protect the confidentiality of health information.[145] If Congress did not meet this deadline, then by default it authorized the Department of Health and Human Services (HHS) to promulgate regulations within six months thereafter (February 2000).[146]

Congress missed its deadline, but not for want of trying to come up with an acceptable package of health privacy laws.

---

140. *See Privacy: Eighth Circuit Says ADA Confidentiality Rules Protect All Employees, Not Just Disabled*, Health L. Rep. (BNA) (Aug. 26, 1999).

141. *See, e.g.*, Jaffee v. Redmond, 518 U.S. 1 (1976) (recognizing, in a limited ruling on the confidentiality of psychotherapists' records, a testimonial privilege against compelling the disclosure of communications between patients and psychotherapists (including social workers) in court proceedings); Whalen v. Roe, 429 U.S. 589 (1976).

142. *See* James G. Hodge, Jr. et al., *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 JAMA 1466, 1468 (1999).

143. *See id.*; *see also Whalen*, 429 U.S. at 600-04 (holding no unconstitutional deprivation of right or liberty by New York statutes that required reporting to state agencies of certain prescription drug information); Gostin, *supra* note 136, at 495-98 (collecting cases that illustrate judicial deference to government's need to acquire and use information about individuals).

144. Pub. L. No. 104-191, 110 Stat. 2021 (1996).

145. *See* Pub. L. No. 104-191, § 264(c)(1) (codified at 42 U.S.C. § 1320d-2 (Supp. 1998)).

146. *See id.*

Every year since 1996, numerous congressional hearings have been held, and many proposed bills have been introduced in Congress.[147] Last summer before the August deadline, five proposed bills were pending in the House of Representatives, and three were pending in the Senate.[148] From February through April of 1999, Senate and House Committees held extensive hearings on proposed legislation, offering testimony from a wide range of consumer, professional, scientific, and industry groups.[149] Still, the deadline came and went.

Complying with HIPAA's default provisions, HHS issued a proposed rule in November 1999, and after receiving more than 52,000 comments on it, HHS issued the final rule in December 2000.[150] The final rule has the force of law and will be enforced by the HHS Office for Civil Rights.[151] The final rule represents a good start toward comprehensive federal protection for patient privacy, but it is necessarily more limited than would be legislation passed by Congress. Even Donna Shalala, Secretary of HHS, and President Bill Clinton did not consider rule-making to be a satisfactory long-term substitute for comprehensive legislation that could, and preferably would, be enacted by Congress in the future.[152]

---

147. *See* Sue Blevins, *Medical Privacy Invasion?*, WASH. TIMES, July 22, 1999, at A17, *available at* 1999 WL 3090419.

148. Copies and comparisons of these various bills are available through the Web sites of several organizations, including the Health Privacy Project of Georgetown University (text of bills) http://www.healthprivacy.org/; the National Coalition for Patients Rights (legislative scorecards) http://www.nationalcpr.org/; and the American Health Information Management Association (analyses of bills) http://www.ahima.org/dc/index.html.

149. *See* Blevins, *supra* note 147.

150. *See* Press Release, U.S. Dep't of Health & Human Servs., HHS Announces Final Regulation Establishing First-Ever National Standards To Protect Patients' Personal Medical Records (Dec. 20, 2000), *available at* http://aspe.hhs.gov/admnsimp/final/press2.htm [hereinafter HHS Press Release]; *see also* Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164, as corrected by Technical Corrections to Final Rule, 65 Fed. Reg. 82944 (Dec. 29, 2000)) [hereinafter Final Rule]. The final rule is available in PDF, text, and HTML format at http://aspe.hhs.gov/admnsimp/index.htm. The compliance date is February 23, 2003 (Feb. 26, 2004, for small health plans).

151. *See* Statement of Delegation of Authority, 65 Fed. Reg. 82381 (Dec. 28, 2000); HHS Press Release, *supra* note 150.

152. *See* HHS Press Release, *supra* note 150; Remarks by the President on Medical Privacy (Dec. 20, 2000), *available at* http://aspe.hhs.gov/admnsimp/final/whpress2.htm.

Shortly after President George W. Bush took office, his administration issued a directive to delay the effective dates of a number of regulations issued in the waning days of the Clinton Administration.[153] The impact of this directive on the HIPAA privacy rule is not clear, and some suggest that the Bush Administration would have to follow the entire administrative rule-making process (including notice of proposed changes and opportunity for comment) if it wanted to make any changes to the new rule.[154]

Industry and public reaction to the new HIPAA rule has been mixed, and privacy advocates and industry representatives on all sides of the debate have found much in the final rule both to praise and to criticize.[155] Privacy advocate Janlori Goldman, for example, has hailed the new rule as strengthening privacy protections and providing a "powerful new tool to stop workplace discrimination."[156] The Health Privacy Project, directed by Ms. Goldman, has summarized many of the key provisions of the final rule, and while finding many improvements over the proposed rule, this privacy advocacy group has expressed concerns about, among other things, "loopholes" in the marketing and fund-raising provisions, weakening of disclosure restrictions for treatment, and inadequate privacy protection of patient records from access by law enforcement officers.[157] Other privacy advocates have expressed concern over the marketing provisions, which they

---

153. *See Regulation: Industry Up in Air on Impact of Bush Directive on Health Care Rules*, Health Law Rep. (BNA) (Jan. 25, 2001) [hereinafter *Industry Up in Air*]. The directive was issued through a memorandum from President Bush's Chief of Staff, Andrew Card, and published in 66 Fed. Reg. 7702 (Jan. 24, 2001). Some argue that the directive will not affect the effective date of the final privacy rule (Feb. 26, 2001) or the dates for compliance (Feb. 26, 2003, generally, and Feb. 26, 2004, for small health plans). *See* Health Privacy Project, Georgetown University, *Presidential Moratorium on Pending Regulations—Does It Affect the Health Privacy Regulation?*, *at* http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=46825 (Jan. 24, 2001).

154. *See Industry Up in Air*, *supra* note 153.

155. *See generally Privacy: Industry, Legislators to Push for Changes to Newly Announced HIPAA Privacy Rules*, Health Law Rep. (BNA) (Jan. 4, 2001).

156. Health Privacy Project, Georgetown University, *Landmark Health Privacy Law Issued by Clinton Administration*, *at* http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=43790 (Dec. 20, 2000).

157. *See* Health Privacy Project, Georgetown University, *Summary of New Federal Health Privacy Regulations*, *at* http://www.healthprivacy.org/newsletter-url2305/newsletter-url_show.htm?doc_id=33936 (last visited Jan. 27, 2001).

say permit disclosure of patient records to pharmaceutical firms and other firms doing business with the patient's providers (although patients can ask to be removed from the mailing list after they have received mailings).[158] Says Robert Gellman: "This is the most anti-privacy and anti-consumer rule I've seen in more than 20 years."[159] The ACLU has called the new rule a "major advance" in privacy protection, but cautions that some of the provisions remain "flawed," especially those involving access by law enforcement officers to patient records.[160]

Industry representatives have been equally quick to respond to the new rule. The President of the Healthcare Leadership Council, Mary Grealy, complained that "[t]he regs will result in more paperwork and higher co-payments and premiums, without improving patient care."[161] The American Association of Health Plans said that "[b]y creating barriers to health information, this rule threatens the effectiveness of programs that promote health and better care for the chronically ill."[162] Some medical researchers are worried that the provisions governing access to patient records for scientific research are "subjective," "proscriptive," and "burdensome."[163] The ERISA Industry Committee, representing the interests of employers' health benefits plans, adamantly warned that the new rule "will subject employers to unworkable rules and litigation hazards and severely cripple employers' ability to operate their health plans and provide employees with disease management and other employee assistance programs."[164]

---

158. *See* Dana Hawkins, *Medical Privacy Rules Give Patients and Marketers Access to Health Data*, U.S. NEWS & WORLD REP., Jan. 29, 2001, *available at* http://www.usnews.com/usnews/issue/010129/nycu/medprivacy.htm.

159. *Id.*

160. Press Release, American Civil Liberties Union, ACLU Says New Medical Privacy Regulations, While Not Perfect, Represent Major Advance in Struggle to Protect Confidentiality (Dec. 20, 2000), *available at* http://www.aclu.org/news/2000/n122000a.html.

161. Hawkins, *supra* note 158.

162. Press Release, American Association of Health Plans, AAHP Statement on New Privacy Rule Issued by HHS (Dec. 20, 2000), *available at* http://www.aahp.org.

163. *Privacy: HHS Regulation May Present New Challenges for Medical Researchers*, Health Law Rep. (BNA) (Jan. 18, 2001) (quoting David Korn, senior vice president for biomedical research at the American Association of Medical Colleges).

164. Press Release, The ERISA Industry Committee, Undoable Medical Privacy Rules Pose Major Threat to Voluntary, Employment-Based Health Care System (Dec. 20, 2000), *available at* http://www.eric.org/press/122000.htm.

D. Sticking Points in Enacting Federal Legislation

With such sharply divergent reactions to the final rule, it is understandable that congressional debates have been equally contentious. But what exactly has been the hang-up in enacting federal legislation? Why has it been so hard to get congressional consensus? And why did it take so long for HHS to promulgate a rule after Congress failed to act?

About a half dozen policy questions have apparently proven intractable in the congressional debates. Efforts to compromise on these sticking points have simply met with little or no success in Congress. Not surprisingly, many of the issues described earlier, which make it difficult to agree upon the right trade-offs in the ethical balancing between individual interests in privacy and social benefits from disclosure, are the same issues which have been the stumbling blocks to enacting comprehensive federal legislation. These issues reflect the ethical tensions in deciding, for example, what is the role that express, informed patient consent to disclosure should play in medical research, law enforcement, health plan operations, and other socially beneficial activity. Other sticking points reflect more formal legal wrangling, such as the debates over whether a new federal law should preempt state privacy laws and whether citizens should be granted a private civil right to sue for violations of their privacy.[165]

Aside from the principles, of course, there is also the question of money. Much of this debate is not just a matter of reconciling conflicts among competing ethical values; these debates are imbued with high financial stakes. How much is privacy worth in actual dollars? Federal officials have estimated that it will cost the industry around $3.2 billion to come into compliance with the HHS regulations in the first year, while industry officials estimate many times that amount.[166] Those people who

---

165. *See* Congressional Research Service, Library of Congress, *CRS Issue Brief: Medical Records Confidentiality* (Oct. 27, 1999) (comparing proposed bills on key controversial issues); *see also* National Committee on Vital Health Statistics, *Health Privacy and Confidentiality Recommendations* (June 25, 1997) (discussing key issues in context of recommendations to the HHS), *available at* http://www.ncvhs.hhs.gov/privrecs.htm [hereinafter NCVHS, *Recommendations*].

166. *See Cost of Privacy Rules Underestimated, AHA Says*, Health Law Rep. (BNA) (Jan. 4, 2001) (citing an American Hospital Association report estimating compliance costs for industry over the next five years to be as much as $22.5 billion). HHS estimates

have had relatively unimpeded access to patient information over the years naturally resist any new obstacles placed in their paths. While their objections may be couched in principled terms—their free access to patient information has been good for the patient, good for other patients, or good for society as a whole—it is also true that many of them have profited from such access as well.

1. Federal Preemption of State Laws

To non-lawyers the preemption issue may seem a bit arcane, but it has been a real flash point in the debates. The issue is whether federal law should provide only a floor of privacy protection by preempting (displacing or superseding) all weaker state privacy laws but not preempting any stronger state privacy protections, or whether federal law should provide floor and ceiling privacy protection by completely preempting *all* state privacy laws in order to provide a single, uniform, and comprehensive national law on health information privacy.

Industry groups (and Republicans) have supported complete preemption, arguing that being subjected to fifty states' extensive and inconsistent laws on privacy is costly and impractical.[167] Additionally, they have argued that patient information flows across state lines because patients often cross state borders to obtain health care such that treatments, consultations, follow-ups, and payments often are not transacted in a single state.[168] One comprehensive federal law would provide much-needed uniformity and predictability, according to such groups as the American Health Information Management Association,[169] the American Public Health

---

the cost of compliance with the final rule to be $17.6 billion over ten years, with a first-year estimate of $3.2 billion. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82760; *see also* U.S. Dep't of Health & Human Servs., Protecting the Privacy of Patients' Health Information: Summary of the Final Regulation, *at* http://aspe.hhs.gov/admnsimp/pvcfact1.htm (Dec. 20, 2000) [hereinafter Summary of the Final Regulation].

167. *See* Geri Aston, *Battle Lines Drawn Over Bills on Medical Records Privacy*, AM. MED. NEWS, May 10, 1999, at 1, *available at* http://www.ama-assn.org/sci-pubs/amnews/pick_99/pick0510.htm.

168. *See* American Health Info. Mgmt. Ass'n, *Confidentiality of Medical Records: A Situation Analysis and AHIMA's Position*, *at* http://www.ahima.org/infocenter/current/white.paper.html (last visited Sept. 11, 2000).

169. *See id.*

Association,[170] and the Health Insurance Association of America.[171] Medical researchers also have supported complete preemption to ensure consistent national rules on access to patients' medical records.[172]

Consumer groups (and Democrats) have supported floor preemption, but have opposed preemption of stronger state privacy laws.[173] States may have tougher privacy protections than a new federal law on, for example, such sensitive health issues as mental health, sexually transmitted diseases, or genetic testing. If these tougher state laws were preempted, then patients could end up with fewer privacy rights than before the federal law was enacted.[174] Privacy advocates have argued that federal law should provide a baseline of privacy protections nationwide, but states should be allowed to experiment with stricter privacy protections than the federal government may adopt. This sort of floor preemption has also been supported by the American Medical Association,[175] as well as the National Conference of State Legislatures and the National Association of Insurance Commissioners.[176]

The HIPAA final rule provides only floor preemption: The agency's regulations do not displace stronger state privacy laws, so the states will remain free to retain and enact tougher privacy protections.[177]

---

170. *See* Geri Aston, *State Laws Show Mixed Results on Privacy*, AM. MED. NEWS, Aug. 9, 1999, at 6.

171. *See Privacy: HIAA Passes Resolution Urging Congress to Pass Bill Protecting Health Information*, Health Care Daily Rep. (BNA) (Feb. 26, 1999).

172. *See* Association of Am. Med. Coll., *Medical Records Confidentiality: AAMC Position Paper*, Issue Briefs Forum, *at* http://www.aamc.org/advocacy/issues/research/mrcon.htm [hereinafter *AAMC Position Paper*].

173. *See* Aston, *supra* note 167.

174. *See* Aston, *supra* note 170; *see also* Aston, *supra* note 167.

175. *See* Geri Aston, *Delegates Firm Up Privacy Policy*, AM. MED. NEWS, July 12, 1999, at 1, *available at* http://www.ama-assn.org/sci-pubs/amnews/pick_99/gvl10712.htm.

176. *See Privacy: National Groups Urge Congress to Rethink Preemption of State Laws in Privacy Bills*, Health Care Daily Rep. (BNA) (May 12, 1999).

177. *See* Summary of the Final Regulation, *supra* note 166; *see also* Final Rule, *supra* note 150, 65 Fed. Reg. at 82801 (to be codified at 45 C.F.R. § 160.203). The HIPAA rule preempts "contrary" state law unless "more stringent." *Id.*

2. Private Right of Action

Whether individual citizens should be able to sue for violation of any new federal privacy law has been an extremely contentious issue. Democrats and consumer groups have favored creating a private right of action against anyone who violated the federal law, arguing that strong enforcement provisions are necessary and appropriate.[178] Republicans and industry groups have opposed a private right to sue, however, or at least have urged limitations on such a right, such as a cap on damages or application only to "willful" violations.[179] Under HIPAA's enabling provisions, HHS is not authorized to permit private lawsuits for violations, although Secretary Shalala supported enacting a private remedy for violations under federal legislation.[180]

Even if the final rule does not expressly provide a private right of action for violation, some believe that the rule's requirements can be argued to set a new, higher standard of care for the industry, and that breach of this national standard of care could result in tort liability.[181]

Under HIPAA, the Secretary is authorized to impose civil and criminal penalties for violations.[182] For unintentional violations, civil penalties under HIPAA are $100 per violation, up to $25,000 per year, per standard.[183] For knowing violations, criminal penalties are up to $50,000 in fines and one year in prison for obtaining or disclosing protected health information, and criminal penalties are up to $100,000 and five years in prison for

---

178. *See Privacy: Bennett Says Medical Privacy Bill Markup May Not Happen Until September*, Health Care Daily Rep. (BNA) (June 21, 1999) [hereinafter *Bennett Says*]; *see also* Palmer, *supra* note 131.

179. *See Bennett Says*, *supra* note 178; Palmer, *supra* note 131.

180. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82605. Secretary Shalala's Recommendations, which were submitted to Congress on September 11, 1997, called for a private right of action for actual damages and equitable relief to permit individuals to enforce their privacy rights. *See id.*; *see also* Summary of the Final Regulation, *supra* note 166 (noting the need for congressional action to create a private right of action to enforce privacy rights).

181. *See Anticipated Privacy Rule Could Give Tort Lawyers New Weapon, Some Say*, Health Law Rep. (BNA) (Dec. 14, 2000).

182. *See* Health Insurance Portability and Accountability Act § 262 (codified at 42 U.S.C. §§ 1320d-5, -6).

183. *See* Summary of the Final Regulation, *supra* note 166.

obtaining health information under false pretenses.[184] The penalty could be up to $250,000 and ten years in prison if the violator tried to sell the health data for commercial purposes, malicious harm, or personal gain.[185]

3. Access to Minors' Medical Records

Another contentious issue involved who should have access to the medical records of minors.[186] If state laws allow juveniles to seek medical treatment on their own without parental consent, should federal law nevertheless allow parents to see their children's records involving such treatment? For example, many states allow minors to get medical treatment for sexually transmitted diseases, treatment related to contraception and pregnancy (including abortion), and drug or alcohol abuse without getting their parents' consent or perhaps without even their knowledge. Particularly in the abortion context, these state laws relating to minors' medical and privacy rights are highly contentious at the state level. The issue in the federal debates has been whether any new federal law should grant parental access to minors' medical records, or whether it should leave state privacy protections intact.

The HIPAA final rule follows the latter route, so that minors will continue to have whatever privacy and treatment rights the states choose to give them.[187] If parents have the right under state law to see their children's records, then they retain that right. Under the final rule, minors who are allowed by state law to consent to treatment on their own will have the same privacy rights as adults, but the states still retain the underlying authority to decide when minors may consent to treatment without parental involvement and whether parents may see those records.[188]

---

184. *See id.*

185. *See id.*; *see also HHS Privacy Reg Seeks To Protect Subjects in Privately-Funded Studies*, HEALTH NEWS DAILY, Nov. 1, 1999, *available at* 1999 WL 10485071.

186. *See Bennett Says*, *supra* note 178; *see also* Pear, *supra* note 93.

187. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82800 (to be codified at 45 C.F.R. § 160.202 (proviso to definition of "more stringent")), 82806 (to be codified at 45 C.F.R. § 164.502(g)); *see generally id.*, 65 Fed. Reg. at 82500 (preamble); 82582, 82634-35 (comments).

188. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82800 (to be codified at 45 C.F.R. § 160.202 (proviso to definition of "more stringent")), 82806 (to be codified at 45 C.F.R.

4. Access by Medical Researchers

The issue over whether medical researchers should have to get the express informed consent of patients prior to undertaking retrospective medical records research surfaced with a vengeance during the congressional debates. Medical researchers have regarded medical records archives as a very valuable national resource. Citing the Minnesota example and the arguments discussed earlier in this paper, they have viewed requirements for prior patient consent as a threat to scientific progress in terms of excessive cost, burdensome bureaucratic red tape, and the potential for invalid research results through selection bias (for example, by excluding the records of patients who refuse to consent, who cannot be located, or whose express consent cannot be obtained for some other logistical reason).[189] Consequently, they have urged Congress to adopt privacy laws for medical records research that would reflect IRB-like review and would allow researchers to proceed without express informed consent if it were impracticable to get consent and if confidentiality safeguards were in place for the research project.[190] Health plans and pharmacies also have objected to extending IRB protections too broadly by imposing costly confidentiality duties beyond the realm of traditional scientific research projects to reach many routine health care operations, such as outcomes research, disease management programs, or other activities aimed at improving quality of care.[191]

Privacy advocates have supported the idea of expanding the scope of federal laws addressing confidentiality in medical records research, for currently the IRB regulations apply only to federally-funded research. Some have also worried, however, about the apparent weakening of the informed consent principle in IRB protocols concerning waivers, effectively turning

---

§ 164.502(g)); *see generally id.*, 65 Fed. Reg. at 82500 (preamble); 82582, 82634-35 (comments).

189. *See AAMC Position Paper*, *supra* note 172; *AAMC Minnesota Report*, *supra* note 86.

190. *See AAMC Position Paper*, *supra* note 172; *AAMC Minnesota Report*, *supra* note 86.

191. *See* Geri Aston, *Privacy Policy Will Have Impact—Any Way It Ends Up*, AM. MED. NEWS, Mar. 15, 1999.

patients into research subjects without their knowledge.[192] Many privacy advocates believe that IRB protections are weak in principle, have proven weaker in practice, and should be made tougher before being extended to private-sector research projects.[193]

Echoing the views of the scientific community in its formal recommendations to HHS, the National Committee on Vital Health Statistics concluded that "requiring patient consent as a condition of researcher access is impractical and expensive. It would also most likely stop a significant amount of useful investigation. This is not in the health interest of individual patients or the general population."[194] The final rule reflects this position: It would allow health care facilities to disclose health information without patient authorization to researchers whose protocol has been reviewed and approved by an existing IRB or a newly created "privacy board."[195] In effect, the final rule would extend the federal Common Rule to all researchers, whether in federally-funded or private-sector research.[196] Researchers would be allowed to access records without patient consent if the research cannot be "practicably" carried out if individual consent were required; if the disclosures involve no more than "minimal risk" to the research subjects; if the anticipated benefits and importance of the research are reasonable in light of the privacy risks to individuals; and if the research project has adequate confidentiality safeguards.[197]

---

192. *See* Woodward, *Challenges*, *supra* note 90, at 1950 ("The dislike of some researchers for the consent requirement, which is the key to a research subject remaining a research subject rather than becoming a research object, is well known.").

193. *See* Aston, *supra* note 170; *see also Privacy: Medical Records Used in Research Need Greater Protection, Senate Panel Hears*, Health Care Daily Rep. (BNA) (Feb. 25, 1999).

194. NCVHS, *Recommendations*, *supra* note 165, at 10.

195. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82816 (to be codified at 45 C.F.R. § 164.512(i)); *see generally id.*, 65 Fed. Reg. at 82535-38 (preamble), 82689-703 (comments).

196. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82816 (to be codified at 45 C.F.R. § 164.512(i)); *see generally id.*, 65 Fed. Reg. at 82535-38 (preamble), 82689-703 (comments).

197. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82816 (to be codified at 45 C.F.R. § 164.512(i)); *see generally id.*, 65 Fed. Reg. at 82535-38 (preamble), 82689-703 (comments).

5. Access by Law Enforcement Officers

Current federal law does not require federal law enforcement officers to get a search warrant or even to notify patients before getting access to their medical records, nor does it mandate any other procedural or judicial protections.[198] Consumer groups and physician organizations have advocated for new federal privacy laws to create tougher standards before law enforcement officers could get access to patients' medical records. Many doctors are uncomfortable with being asked by police to violate their patients' privacy. They would prefer that police be legally required to go through some judicial review process—for example, get a warrant or other court order—before the doctors are required to release their records to the police.[199] Civil liberties groups have also urged that law officers should have to meet tougher federal standards than at present.[200] The ACLU has argued that, as with other areas of individuals' right to be free from unreasonable government intrusions into their privacy, the police should have to show "probable cause" that a crime has been committed before gaining access to patients' records.[201] The ACLU has also urged that since an individual's privacy in her home is protected under the Fourth Amendment by the requirement of a search warrant before the government can intrude, then medical records in a doctor's office should be given the same protection of prior judicial review.[202]

Law enforcement officers have argued that federal law should maintain the status quo and impose no new privacy protections, such as requiring a court order or other review prior to gaining access to medical records.[203] They have wanted exceptions in the case of health oversight activities, such as fraud and abuse, and

198. *See* Hallam, *supra* note 112; Van Meveren, *supra* note 110.

199. *See Caregivers Walk Fine Line in Aiding Police, Protecting Confidentiality*, 15 MED. ETHICS ADVISOR 85 (1999); *see also* Pear, *supra* note 93 (citing the AMA's position); Palmer, *supra* note 131 (citing American Hospital Association's position).

200. *See* Ronald Weich, on behalf of the ACLU, Medical Records Confidentiality in a Changing Health Care Environment, Testimony Before the Senate Comm. on Health, Education, Labor, and Pensions (Apr. 27, 1999), *available at* http://www.aclu.org/congress/lg042799a.html.

201. *See id.*

202. *See* Alissa J. Rubin, *Privacy Initiative Elicits Praise, Concern*, L.A. TIMES, Oct. 30, 1999, at A12.

203. *See* Hallam, *supra* note 112.

they have wanted to preserve their ability to get immediate access to medical information without a warrant in emergencies, such as bomb threats or hostage rescues.[204] Law enforcers have argued, for example, that they should be allowed to get local hospitals to notify them immediately if a fleeing suspect showed up for treatment of a gunshot wound, or to obtain the health information about someone who is holding hostages or is being held hostage.[205]

Secretary Shalala initially appeared inclined toward the status quo, but the final rule does enact some new protections. HHS has no authority to control local, state, or federal law enforcement officers, but the final rule allows health care facilities to insist upon, in some circumstances, certain minimum legal procedures—for example, a warrant, grand jury subpoena, or administrative subpoena or summons—before having to disclose confidential information during a law enforcement inquiry.[206] At a minimum, an officer would have to seek an administrative subpoena, which is issued internally by the law enforcement agency.[207] The final rule does not require prior approval from a judge or magistrate before the release of records, however, which privacy groups and even the AMA had advocated for.[208]

6. Informed Consent and Patient Authorization

Finally, there has been substantial controversy over the nature of the consent, or authorization, which health insurers and managed-care companies should be required to get from subscriber-patients before using their health information in the course of treatment, payment, and—most controversially—other

---

204. *See* Van Meveren, *supra* note 110.

205. *See id.*; *see also* Robert Pear, *Clinton To Stress Medical Privacy: Regulations on Confidentiality of Records To Be Proposed Soon*, SAN DIEGO UNION-TRIB., Oct. 27, 1999, at A1.

206. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82815 (to be codified at 45 C.F.R. § 164.512(f)); *see generally id.*, 65 Fed. Reg. at 82531-34 (preamble), 82678-87 (comments).

207. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82815 (to be codified at 45 C.F.R. § 164.512(f)); *see generally id.*, 65 Fed. Reg. at 82531-34 (preamble), 82678-87 (comments).

208. *See* Dawn MacKeen, *The Medical Privacy Debate: Do Clinton's New Guidelines Go Far Enough?*, *at* http://www.salon.com/news/feature/2000/12/21/medical/index.html (Dec. 21, 2000).

"health care operations."[209] Current practice is for health plans to get a signed blanket authorization form from subscribers allowing them pretty much to do anything reasonably foreseeable with their records. Some of the proposed federal bills made the granting of such authorization a condition of enrollment in the plan: If the subscriber would not give such blanket authorization upon enrollment for use of his records in the future, the health plan would not be required to sign him up.[210]

Consumer and physician groups have opposed this practice as "coerced consent"—forcing patients to consent to widespread disclosures of their medical information on penalty of losing their health insurance.[211] While patients might be asked to consent broadly to disclosures related to treatment and payment, privacy advocates have asserted that express, specific consent should be required for "other health care operations."[212] The industry in turn has vociferously complained that it would be impossibly inefficient and unbearably bureaucratic to go back to each patient for each additional use beyond payment and treatment. Such a burdensome requirement, industry opponents have argued, would impede their efforts to improve quality of care and control costs through such activities as disease management programs and coordinating care across health systems.[213]

The final rule requires health care providers to obtain patient "consent" before using or disclosing patient information to carry out "treatment, payment, or health care operations."[214] With respect to "health care operations," express patient consent to disclosure of the information in their medical records is now necessary for, inter alia, quality assessment, developing clinical guidelines, training, review of professional competence, accreditation, legal services, and auditing functions (including

209. *See* Janet Gemingnani & Nancy Rowell, *Privacy Prompts Partisan Scuffle*, BUS. & HEALTH, July 1, 1999, at 8.
210. *See id.*
211. *See id.*
212. *See* Aston, *supra* note 167.
213. *See* NOTHING SACRED, *supra* note 23, at 33-37; *see also* Aston, *supra* note 167.
214. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82810-11 (to be codified at 45 C.F.R. § 164.506); *see generally id.*, 65 Fed. Reg. at 82509-13 (preamble), 82648-50 (comments).

fraud and abuse compliance).[215] A controversial provision of the final rule allows a health care provider to condition its provision of treatment on the patient's giving consent to its use or disclosure of health information.[216] Consumer advocates have referred to this provision as "sign or die."[217] However, HHS justifies it on the ground that "it would be difficult, if not impossible, for health care providers to treat their patients and run their businesses without being able to use or disclose protected health information for these purposes" (for example, to obtain reimbursement for the treatment from a health plan).[218] Similarly, a health plan may condition enrollment in the health plan on the patient's giving consent to information disclosure, if consent is sought in conjunction with the enrollment process.[219]

Under the final rule, "consent" is distinguished from "authorization." "Consent" is written permission for uses and disclosures of health information to carry out treatment, payment, and health care operations.[220] Most persons who obtain "consent" will be health care providers, and such "consent" is limited to use or disclosure only by the entity obtaining the consent, not by other persons.[221] "Authorization" is written permission, in specific terms, for uses and disclosures of health information for purposes other than treatment, payment, and health care operations, and by third parties other than the entity obtaining the authorization.[222] For example, authorization generally must be obtained for purposes of marketing, pre-enrollment underwriting, employment determinations, fund-raising, and use of psychotherapy notes.[223] Privacy advocates, however, have identified the marketing

---

215. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82803 (to be codified at 45 C.F.R. § 164.501 (defining "health care operations")).
216. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82810 (to be codified at 45 C.F.R. § 164.506(b)(1)); *see generally id.*, 65 Fed. Reg. at 82511 (preamble), 82649 (comments).
217. Hawkins, *supra* note 158.
218. Final Rule, *supra* note 150, 65 Fed. Reg. at 82649 (comments).
219. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82810 (to be codified at 45 C.F.R. § 164.506(b)(2)); *see generally id.*, 65 Fed. Reg. at 82511 (preamble), 82649 (comments).
220. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82509 (preamble).
221. *See id.*
222. *See id.*, 65 Fed. Reg. at 82509-10 (preamble), 82650-62 (comments).
223. *See id.*, 65 Fed. Reg. at 82513-15 (preamble).

provisions[224] in particular as being "significant and troublesome loopholes"[225] in privacy protection.

In addition, the final rule provides that individuals have a right to "notice" of the privacy practices of the covered entity, informing individuals of the uses and disclosures that may be made of their health information and advising them of their rights with respect to their health information.[226] The form providing this "notice" must be made a separate document from the "consent" form.[227] As a practical matter, this notice form could become quite lengthy in light of the final rule's extensive required elements for its content.[228]

7. Other Provisions in the Final Rule

The final rule protects *all* medical records and other "identifiable health information . . . in any form, whether communicated electronically, on paper, or orally."[229] This differs substantially from the proposed regulations, which covered only electronic records, but not paper or oral records which had never existed in electronic form.[230]

An inherent limitation in the final rule is that it does not cover everyone who holds patient information. The rule covers health information only in the hands of specified "covered entities": health plans, health care providers who transmit any health information in electronic form, and health care clearinghouses (entities that process health information between provider and health plan, e.g., billing).[231] Entities that are not "covered" include a multitude of entities who may receive health information from a covered entity in the course

---

224. *See id.*, 65 Fed. Reg. at 82804 (to be codified at 45 C.F.R. § 164.501), 82819-20 (to be codified at 45 C.F.R. § 164.514(e); *see generally id.*, 65 Fed. Reg. at 82545-46 (preamble), 82716-18 (comments).

225. *Summary of New Federal Health Privacy Regulations*, *supra* note 157, at 5; *see also* Hawkins, *supra* note 158; Robert O'Harrow Jr., *Patient Files Opened to Marketers, Fundraisers*, WASH. POST, Jan. 16, 2001, at E1.

226. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82820 (to be codified at 45 C.F.R. § 164.520); *see generally id.*, 65 Fed. Reg. at 82547-52 (preamble), 82720-26 (comments).

227. *See id.*, 65 Fed. Reg. at 82810 (to be codified at 45 C.F.R. § 164.506(b)(3)).

228. *See id.*, 65 Fed. Reg. at 82821 (to be codified at 45 C.F.R. § 164.520(b)).

229. Summary of the Final Regulation, *supra* note 166.

230. *See id.*

231. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82798 (to be codified at 45 C.F.R. §§ 160.102-160.103).

of business dealings with it, such as "business associates" who perform legal, actuarial, accounting, consulting, financial, or other services for the covered entity but who are not members of the covered entity's workforce.[232] Because HIPAA authorized HHS to make rules only for health plans, clearinghouses, and providers, but not for the many entities who might receive information from them, the regulations could not directly regulate how these other entities might use or re-disclose information they received from a covered entity.[233]

HHS addressed this regulatory gap through "business associate" contracts.[234] The final rule requires that all the business associates of a covered entity be contractually bound not to use or further disclose information in a way that would violate the rule if done by the covered entity.[235] Moreover, the covered entity will be held accountable for any business associate's material breach of the contract that the covered entity knew about, unless the covered entity took reasonable steps to cure the breach or end the violation.[236] These "business associate" contracts allow HHS to extend the regulatory privacy protections beyond the covered entities it was directly authorized to regulate. Congressional legislation would not face such restrictions and could cover directly all entities who hold health information, which is one reason HHS continues to prefer passage of federal legislation to its own regulations.[237]

Other highlights of the regulations include a number of fair information practices. Patients are given new federal rights of access to inspect and copy and to request corrections to their medical records.[238] Moreover, individuals have a right to receive an accounting of all instances in which their information was

---

232. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82798 (to be codified at 45 C.F.R. § 160.103 (definition of "business associate")), 82475-76 (preamble).

233. *See generally* Final Rule, *supra* note 150, 65 Fed. Reg. at 82503-07 (preamble), 82640-45 (comments).

234. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82503-07 (preamble).

235. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82808 (to be codified at 45 C.F.R. § 164.502(e)), 82808 (to be codified at 45 C.F.R. § 164.504(e)).

236. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82808 (to be codified at 45 C.F.R. § 164.504(e)(1)), 82503-07 (preamble).

237. *See* Summary of the Final Regulation, *supra* note 166.

238. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82823-26 (to be codified at 45 C.F.R. §§ 164.524, 164.526); *see generally id.*, 65 Fed. Reg. at 82554-59 (preamble), 82731-38 (comments).

disclosed for purposes other than treatment, payment, or health care operations.[239] Health plans, providers, and clearinghouses are also required to make reasonable efforts to limit protected health information to the "minimum necessary" to accomplish the intended purpose of the use or disclosure.[240] This restriction does not apply to disclosures for the purposes of treatment.[241]

The final rule requires providers and health plans to maintain administrative, technical, and physical safeguards to protect confidentiality and protect against unauthorized access.[242] For example, covered entities are required to designate a "privacy official" within the institution to develop policies and procedures concerning use and disclosure of health information; to provide training to members of the institution's workforce about its privacy policies; to develop administrative, technical, and physical safeguards against any intentional or unintentional use or disclosure in violation of the rule; to develop a complaint mechanism for the institution's privacy policies and procedures; and to impose disciplinary sanction for violations by members of the institution's workforce.[243] These safeguards may appear largely bureaucratic, but the final rule seems to provide discretion to health care institutions as to how to implement these safeguards, which may be key to developing a strong culture of privacy within the institution.

---

239. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82826 (to be codified at 45 C.F.R. § 164.528); *see generally id.*, 65 Fed. Reg. at 82559-61 (preamble), 82739-44 (comments).

240. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82805-06 (to be codified at § 164.502(b)), 82819 (to be codified at 45 C.F.R. § 164.514(d)); *see generally id.*, 65 Fed. Reg. at 82543-44 (preamble), 82712-16 (comments).

241. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82805 (to be codified at 45 C.F.R. § 164.502(b)(2)(i)), 82712-13 (noting that many commentators had objected to limiting disclosures to "minimally necessary" ones in the treatment situations, where "caregivers need to give and receive a complete picture of the patient's health to make a diagnosis and develop a treatment plan").

242. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82826-28 (to be codified at 45 C.F.R. § 164.530); *see generally id.*, 65 Fed. Reg. at 82561-64 (preamble), 82744-50 (comments).

243. *See* Final Rule, *supra* note 150, 65 Fed. Reg. at 82826-28 (to be codified at 45 C.F.R. § 164.530); *see generally id.*, 65 Fed. Reg. at 82561-64 (preamble), 82744-50 (comments).

CONCLUSION

> "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasions of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding." – Justice Louis D. Brandeis[244]

Your privacy is a lot like your reputation—once you lose it, it is very difficult to get it back. Both the ethical tensions and the legal debates have entailed considerable balancing of an individual's interest in privacy against other larger concerns of the community. Have our social ends in the promotion of public health, safety, and welfare too quickly justified the means of sacrificing personal privacy? Some have thought so. Beverly Woodward, a Brandeis University sociologist, has worried that at times "it has seemed that individual privacy will get balanced right out of existence."[245] During the debates on the proposed legislation, Richard Sobel, a research fellow at Harvard University, commented, "I'm afraid the compromise bill will compromise privacy.... You can't have just a little bit of privacy protection."[246]

Overall, the argument that too much privacy is bad for our collective health has been a pretty successful one. We have often been persuaded that maintaining privacy was not in the patient's or in the public's best interest. We have often agreed that letting the *patient* control who has access to his health information would be, for example, bad for the health of the individual patient (by preventing MCOs or PBMs from ensuring that the care she receives is appropriate and cost effective); bad for the health of other patients (by threatening scientific advances through medical records research); bad for the health and safety of other people (by obstructing public health reporting and surveillance measures); bad for the American public in general (by impeding law enforcement efforts); and bad for the viability of the American health care system as we

244. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).
245. Allen, *supra* note 4.
246. Palmer, *supra* note 131.

know it (by derailing efforts to improve its quality and lower its costs).

Perhaps the ethical and legal trade-offs have been the right ones, as surely many people would argue. I would like to make a few cautionary observations, however. First, as Justice Brandeis warns, we should be wary when someone (especially government) tells us that they are doing something for our benefit, that "it's for our own good" that we are being asked to give up something that was ours, be it our liberty, our property, or our privacy.

Second, we should be wary when someone—not the patient—argues that it is too much trouble—too costly, too burdensome, too impractical—to ask the patient what she or he would prefer to do. Medical researchers, HMOs, law enforcement officers, public health officials, and others all strenuously argue that it is just too much trouble to get the patient's voluntary and informed consent before they look at the patients' records. The potential problem with this argument is that we have heard it before, in contexts that now we look back on and think how wrong it was not to have gotten the patient's consent at the outset. For example, physicians long resisted any duty to obtain the patient's informed consent to treatment, on the grounds either that they (the doctors) knew what was in the patient's best interest, or that requiring consent might impede the treatment itself (the patient might refuse). Yet now there is general societal consensus that, ethically speaking, it is the patient's right, not the doctor's, to decide what treatment the patient should have. The law in every state now reflects this ethical view by requiring that patients be given the opportunity to be informed about, to consent to, or to refuse medical treatment before it is rendered.

Moreover, the history of human subject research in this country should remind us of the price paid by sacrificing the informed consent principle too quickly. There are numerous examples of scientific experiments in which researchers deliberately failed to obtain the prior consent of the human subjects who were studied, such as the infamous Tuskegee Syphilis Study or the Cold War radiation experiments. These activities are now regarded as clear abuses of individual rights rather than celebrated for any scientific achievements or other social goods that may have originally motivated their sponsors.

Finally, rather than being bad for your health, assurances of privacy may be the most important foundational element for promoting good health. As was discussed earlier, studies have shown that patients often engage in "privacy-protecting behaviors"—such as withholding information from their doctors, getting doctors to compile incomplete or inaccurate records, going to several doctors, or avoiding health care altogether. These behaviors can threaten both the doctor-patient relationship and the quality of health care provided. Assuring privacy within the doctor-patient relationship encourages full and open dialogue, which is essential to appropriate diagnosis and treatment. Trust may well be the first premise of high-quality health care.[247]

Along this line, the United States Supreme Court has recognized that privacy laws which promote an individual's health also promote the public interest. In the context of requiring that communications between psychotherapists and patients be kept confidential, no matter what bearing they may have in the search for truth in court proceedings, the Court observed: "The psychotherapist privilege serves the public interest by facilitating the provision of appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance."[248] Rather than being at odds with societal welfare, strong legal protections for individual privacy may prove to be critical, in the long run, to safeguarding our public health.

247. *See* Goldman, *supra* note 57, at 47-60.
248. Jaffee v. Redmond, 518 U.S. 1, 11 (1996).