Vanderbilt Law Review

Volume 48
Issue 2 *Issue 2 - March 1995*

Article 1

3-1995

The Protection of Privacy in Health Care Reform

Paul M. Schwartz

VANDERBILT LAW REVIEW

VOLUME 48 MARCH 1995 NUMBER 2

The Protection of Privacy in Health Care Reform

*Paul M. Schwartz**

* Associate Professor of Law, University of Arkansas (Fayetteville); Visiting Scholar, Columbia University School of Law (Summer 1994).

This Article is a revised and expanded version of testimony delivered before the Government Information, Justice, Transportation and Agriculture Subcommittee of the Government Operations Committee of the House of Representatives. I wish te thank Representative Gary Condit, for the opportunity to spoak before the Subcommittee.

I also wish to thank Jutta Körbel, Spiros Simitis, Joel R. Reidenberg, Laura Schwartz, Joseph Goldstein, John Applegate, Martin Flaherty, Robert Gellman, Jim Bennett, and Bill Treanor who made insightful comments on earlier drafts. David Gay and Anne Arendt offered excellent bibliographic help, and Terri Yeakley her impeccable administrative skills. Christine Dodd provided superb research assistance. Finally, I am grateful to Dean Lance Liebman of the Columbia University School of Law for his invitation to share in the stimulating environment at West 116th Street.

I. INTRODUCTION

Legal regulation of the privacy of medical information is now at a critical stage. Americans are highly concerned about the processing and use of their personal data. Over three-quarters of the public currently believes that the individual has lost control of how personal information is circulated and applied by companies.[1] Indeed, a recent poll reveals that those who know the most about the current protection of medical information—physicians, heads of medical societies, health insurers, and hospital CEOs—are also the most concerned about threats to personal privacy.[2]

Social concern about the threat to informational privacy has resulted in strong approval for the creation of detailed protections for medical information.[3] Support for increased protection is well justified; current regulation of health care data is not successful. Moreover, the flaws in the existing legal structure will be exacerbated by inevitable increases in the demand for personal medical information. In particular, many current proposals for health care reform seek to increase access to personal medical information for a host of entities as a means to control medical costs, improve the provision of medical services, and further scientific research. This increased access will occur through continued computerization of health care data and through opening access to personal medical information.

---

1. See Harris-Equifax, *Health Information Privacy Study* 2, 33 (1993) ("*Health Information Privacy Survey*") (stating that eighty percent of the American population is very or somewhat concerned about threats to its personal privacy). These concerns about privacy cut across all demographic subgroups within American society. Id. at 22-33.
2. Alan Westin, *Interpretive Essay*, in *Health Information Privacy Study* at 22.
3. *Health Information Privacy Study* at 97-103.

This Article argues that health care reform and marketplace changes in health care services should be accompanied by improvements in the protection of health care information. Part II of this Article discusses the weaknesses of current regulation of the use of personal medical data. Perhaps the most striking indication of these shortcomings is the sale by direct market mailers of lists of individuals suffering from certain diseases or conditions.[4]

The insufficiency of current legal regulation is further demonstrated by employer access to personal medical information of employees through corporate wellness programs or employer-managed health insurance plans.[5] Although most workers believe that such health care data are confidential, employers may use the information in ways detrimental to employees, including opposing worker's compensation claims, shifting health care costs to employees with unhealthy lifestyles, and discouraging litigation by employees who are slated to lose their jobs.[6] These abuses may not be corrected by proposed health care reform. For example, the Clinton health program, which aggressively promoted the dissemination of medical information and encouraged the establishment of wellness programs, failed to make adequate provisions for redressing existing weaknesses in the regulation of health care data.[7]

Part III of this Article offers another reason for improvements in this area of law. It introduces a comparative perspective by examining significant European developments in data protection law. The term "data protection" refers to the area of law that governs the collection, storage, and use of personal information.[8] Data protection regulations represent an ongoing balance between the need for privacy and for the use of personal information. Europe's generally high standards of data protection not only provide a positive example, but also a potential threat, to the United States. European law allows

---

4. See notes 90-92 and accompanying text.

5. See notes 34-35 and accompanying text.

6. See notes 79-82 and accompanying text.

7. See notes 151-53 and accompanying text. To be just to the Clinton health program, I must add that the original Health Security Act, even if imperfect, did reflect an awareness of and willingness te address the issue of privacy protoction. Moreover, as the debate regarding health care reform developed during the 103d Congress, the Clinton Administration proved responsive to demands for additional privacy in health care information and supported the Fair Health Information Practices Act of 1994, which I discuss at notes 257-60 and accompanying text.

8. See generally Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell U., 1992); David H. Flaherty, *Protecting Privacy in Surveillance Societies* (U.N.C., 1989); Paul M. Schwartz, *Data Processing and Government Administration*, 43 Hastings L. J. 1321 (1992).

states to block the transfer of personal information to those with insufficient data protection.[9] As a result, weaknesses in the regulation of health care information threaten United States access to international data flows. These European restrictions are likely to have a highly negative impact on American corporations that compete globally for contracts that involve the processing of health information.[10] Both the weaknesses in the current American approach and the developments in Europe offer strong grounds for the creation of federal standards of fair information practices for health care in the United States.

Part IV considers the nature of the needed federal standards. The core of fair information practices that should be applied to medical information are: (1) the creation of a statutory fabric which defines obligations with respect to the uses of personal information; (2) the maintenance of transparent processing systems; (3) the assignment of limited procedural and substantive rights to the individual; and (4) the establishment of effective governmental oversight of data use. This Article develops these four jurisprudential principles and suggests how they should be applied in an American data protection law to combat existing weaknesses in the regulation of American medical privacy.

II. THE PROTECTION OF HEALTH CARE DATA

A. Data Processing and Medicine

1. Health Policy Considerations

The Clinton Administration has committed itself to national health care reform. Its initial approach, as expressed in the Health Security Act of 1993, involved global budgets for health care expenditures, the creation of regional health care alliances, and universal coverage for all Americans.[11] Regardless of what reform, if any,

---

9. See notes 194-218 and accompanying text.

10. See note 211 and accompanying text.

11. Health Security Act of 1993, H.R. 3600, S.1757, 103d Cong., 2d Sess. (Nov. 20, 1993) §§ 1001-1006, 1131-1136, 1301-1306, in 139 Cong. Rec. E2571 (daily ed. Oct. 28, 1993) ("Health Security Act"). An official explanation of this Bill is offered by The White House Domestic Policy Council, *Health Security: The President's Report to the American People* 21-27 (Oct. 1993) ("*Health Security Report*"). For a discussion of the Administration's plan by a Clinton advisor,

Congress eventually enacts, important health care reform is already taking place and will continue in the immediate future. Some change is taking place through modifications of legal regulations at the state level;[12] other transformations are being shaped by the private sector.

Two policy issues are driving this reform: the scope of coverage and the increased costs of health care. On one hand, the sharply rising cost of health care threatens the economic prosperity of the United States. As one political scientist has stated, "Simply put, society cannot afford to fulfill the insatiable medical demands of the population."[13] A piecemeal system of allocating social spending for medical care has failed to set adequate limits on the cost of these services.[14] On a more individual and immediate level, millions of citizens are now worried about the current system of employment-based health insurance, fearing that an unexpected loss of employment or the development of certain diseases or conditions will leave them uninsured or uninsurable and, thus, unprotected from ruinous health care costs.[15]

---

see Paul Starr, *The Logic of Health Care Reform: Why and How the President's Plan Will Work* (Whittle, rev. ed. 1994). See also Ronald Dworkin, *Will Clinton's Plan Be Fair?*, 41 N. Y. Rov. of Books 20, 22 (Jan. 13, 1994) (developing "prudent insurance" principle to decide that Clinton health reform proposal is fair); Uwe E. Reinhardt, *Universal Coverage. It's Now or Never*, N. Y. Times A23, A23 (June 29, 1994) (arguing that employer-based universal coverage, as advocated in Clinton's plan, will cut health sponding and provide secure health protection for Americans).

12. For discussions of the states' efforts to provide health reform through improved access to both health care and health insurance, see generally Robert D. Ray and Brian Lester Smith, *Selected Legal Issues Affecting a State's Movement Towards Health Care Reform*, 42 Drake L. Rev. 711 (1993); Robin Toner, *Health Care Battle in California Turns on State Insurance*, N.Y. Times A1 (Sept. 30, 1994); Robort Pear, *States Again Try Health Changes as Congress Fails*, N.Y. Times A1 (Sept. 16, 1994).

13. Robert H. Blank, *Rationing Medicine* 75 (Columbia U., 1988). Although society cannot afford to fulfill all of its population's demands for health care, difficult decisions about the valuation of lives and health complicate any attempt te discuss cost containment. As a leading health economist comments: "That life is priceless need not imply that we will spare no expense to save a life or cure a disease. Yet that myth persists and gives us comfort. . . . Given our need for myths, many mechanisms of cost containment must work in the shadows." Victor R. Fuchs, *The Future of Health Policy* 49 (Harvard U., 1993).

14. In the words of the Clinton White House:

> Between 1980 and 1992, American health care spending rose from 9 percent of Gross Domestic Product (GDP) to 14 percent. Without reform, spending on health care will reach 19 percent of GDP by the year 2000. If we do nothing, almost one in every five dollars spent by Americans will go to health care by the end of the decade, robbing workers of wages, straining state budgets and adding tens of billions of dollars to the national debt.

Health Security Report at 7 (cited in note 11).

15. In a 1993 New York Times poll, more than 30% of Americans stated that they or a member of their family had remained in a job that they wanted to give up or had selected one job rather than another because of health benefits. Erik Eckholm, ed., *Solving America's Health-Care Crisis* 9 (Times Books, 1993). See Dworkin, 41 N.Y. Rev. of Books at 25 (cited in note 11) (stating that "[h]ealth care reform has a reasonable chance of success . . . because so many

The first, unsuccessful attempt at health care reform by the Clinton Administration stressed the first issue, universal coverage, as reflected in the name of the administration's voluminous proposed legislation, the Health Security Act.[16] The theme of the next round of reform efforts will likely be the second issue, the need to cut costs.[17]

2. Privacy Policy Considerations

Whatever reforms are adopted, any changes in the health-delivery system are likely to increase the use and sharing of health care information. Medical data processing will be increasingly relied upon to help reduce waste and fraud, and to increase the efficiency of both the practice of medicine and the payment process.[18] This data processing will raise new threats to the specific privacy interest of patients in informational autonomy. Understanding this risk requires this Article first to consider the nature of health care data processing as it exists and the impact of changes likely under health care reform. Additionally, this Part will examine the nature of the interest in informational autonomy.

a. The Increasing Role of Data Processing in Health Care

Information processing already plays a critical role in the provision, regulation, and financing of medical services by government and private entities. The past social tradition of deference to the medical profession and its self-regulation is silently being replaced by a model of control through data processing.[19] As two physicians have

---

voters are frightened by their prospects under the current system"). But see Fuchs, *The Future of Health Policy* at 216 (cited in note 13) (noting his pessimism about the likelihood of health care reform).

16. See note 11.

17. See *Clinton's Budget Dilemma: Do the Right Thing or the Political Thing?*, Bus. Week 47, 47 (Oct. 24, 1994) (reporting that the President's Chief of Staff "has signaled that the next year's version of health-care reform should be repackaged as a cost-cutting effort rather than an overhaul of the health-delivery system").

18. See notes 31-39 and accompanying text.

19. The notion of replacing deference to the medical profession with policies that lead to new allocations of information first emerged in two contexts in tort law. The first concerned the application of res ipsa loquitur to break conspiracies of silence among medical caregivers. See *Ybarra v. Spangard*, 25 Cal 2d 486, 154 P.2d 687, 691 (1944) (stating "where a plaintiff receives unusual injuries while unconscious and in the course of medical treatment, all those defendants who had any control over his body or the instrumentalities which might have caused the injuries may properly be called upon to meet the inference of negligence by giving an explanation of their conduct"). Here, the law allows an inference of negligence on the part of all the health care givers present during an operation to put pressure on these medical professionals to provide information about what actually happened.

commented in the pages of the New England Journal of Medicine, "Medicine is increasingly a spectator sport."[20] A widening audience of outside observers now watch the performance of doctors, nurses, and patients.

These outside observers, who include both state and private entities, rely on the collection and application of information, including personal data, as a way to control physicians, regulate health care expenditures, and help physicians control patients. This information is no longer exclusively located in the offices of those directly responsible for patient care, but is shared among a wide variety of entities. Alan Westin has made a highly useful description of the flow of personal medical information in the United States today. Westin sets out three zones where information is used: zone one is direct patient care (doctors, clinics, nursing homes); zone two consists of supporting and administrative activities (service payers, third party administrators, quality of care reviewers); and zone three includes broader applications of health data, termed "secondary uses" (credential and evaluation decisions, public health reporting, social welfare programs, direct marketing).[21] More organizations than ever before are seeking—and obtaining—access to health care information. Select examples from the public and private sectors illustrate this trend.

Medicare and Medicaid demonstrate the government's ability to control the practice of medicine through data processing. Medicare is the federal program of health care for the elderly;[22] Medicaid is the joint federal-state program that provides medical services for poor

---

Another area in which tort law limits deference to physicians is the notion of informed consent, see note 48 and accompanying text.

20. Steffie Woolhandler and David U. Himmelstein, *The Deteriorating Administrative Efficiency of the U.S. Health Care System*, 324 N. Eng. J. Med. 1253, 1253 (1991). See Mark A. Hall, *Institutional Control of Physician Behavior: Legal Barriers to Health Care Cost Containment*, 137 U. Pa. L. Rev. 431, 433-36 (1988) (discussing "a revolutionary tranformation . . . in American medicine": implementation of new managerial controls over physician behavior); Lisa Belkin, *Many Doctors See Themselves Drowning in a Sea of Paperwork*, N.Y. Times A1, A1 (Feb. 19, 1990) (noting that the most common reason given by physicians in a Gallup Poll who would not go to medical school if they were in college today was "government or insurance regulations that 'interfere with doing my job' and cause a 'lack of autonomy'").

21. Alan F. Westin, *Interpretive Essay*, in *Health Information Privacy Survey* at 7 (cited in note 1).

22. Medicare is a federal insurance program with two distinct components. Part A is a hospital insurance program that is financed through payroll taxes. 42 U.S.C. § 426 (1988 & Supp. 1990). Part B provides optional supplemental coverage funded by general federal revenues and beneficiary paid premiums. 42 U.S.C. § 1395j et seq. (1988 & Supp. 1993). For an excellent introduction to this complex law, see Lawrence A. Frolik and Alison Patrucco Barnes, *Elderlaw* 307-35 (Michie, 1992).

people.[23] Both programs have engendered bureaucracies that collect and review personal data to decide whether a given patient is eligible for medically necessary services. The decision as to which medical services are necessary, and therefore subject to public funding, rests with these bureaucracies and not with the physician.[24]

The government has also relied on its collection of personal medical information to decide how much it will pay for these medically necessary services. This control is carried out in part through the government's administration of Diagnosis Related Groups, or DRGs, in Medicare.[25] Once a given service is found to be medically necessary, a DRG sets a monetary amount for the prospective reimbursement of treatment. Currently, over four hundred DRGs match the condition or disease of a patient with the reimbursement fee that the federal government will provide.[26] These price controls can only be applied, however, when patient data are subject to outside review. One important kind of such review involves the examination of patient records to guard against so-called "DRG creep," which occurs when physicians place patients into more generous DRG categories than are warranted.[27]

---

23. Medicaid is run by individual states, who receive federal funds that they are required to match. 42 U.S.C. § 1396 (1988). The steep, ongoing rise in health care costs has led to periodic funding crises for Medicaid in individual states. Part of the response to these funding problems has been cuts in services. See, for example, *Benton v. Rhodes*, 586 F.2d 1, 14 (6th Cir. 1978) (stating that "when a state decides to terminate optional [Medicaid] benefits on the basis of lack of appropriated funds, or for any other state reason, this is a matter of state law or policy which it was permitted to adopt"). These crises have also been met with piecemeal attempts at raising additional state revenues. A good example of this ad hoc approach is the tax that Arkansas has placed on soft drinks since 1993 to overcome its difficulties financing Medicaid. Ark. Stat. Ann. §§ 26-57-901 to 26-57-909 (Supp. 1993). Such a tax is, of course, highly regressive in nature.

24. *Sarchett v. Blue Shield of California*, 43 Cal. 3d 1, 729 P.2d 267, 272 (1987); *Cowan v. Myers*, 187 Cal. App. 3d 968, 232 Cal. Rptr. 299, 303 (1986); *Lockshire v. Blue Cross*, 70 Ohio App. 2d 70, 434 N.E. 2d 754, 756 (1980). See Frank P. Grad, *The Public Health Law Manual* 24 (American Public Health Assoc., 2d ed. 1990) (stating that Medicare and Medicaid "brought the government into the field of health care and introduced new regulatory controls into the provision of medical and treatment services").

25. 42 U.S.C. § 1395ww(d) (1988 & Supp. 1993).

26. George J. Annas, Sylvia A. Law, Rand E. Rosenblatt, and Kenneth R. Wing, *American Health Law* 233-60 (Little, Brown, 1990).

27. Charles J. Dougherty, *American Health Care: Realities, Rights, and Reforms* 149-53 (Oxford U., 1988).

Another example of data processing in the context of Medicare and Medicaid is the Health Care Financing Administration's recent attempt to develop a Medicare/Medicaid data bank. The creation of this data bank was authorized by the Omnibus Budget Reconciliation Act of 1993; its purpose is:

> to save millions by strengthening processes to (1) identify the approximately 7 million Medicare and Medicaid beneficiaries who have other health insurance coverage that should pay medical bills ahead of the Medicare and Medicaid programs and (2) ensure that this insurance is appropriately applied to reduce Medicare and Medicaid costs.

A final example of governmental control of the practice of medicine through information processing is the establishment, through federal law, of the National Practitioner Data Bank.[28] This data bank contains reports of malpractice payments and other adverse information regarding physicians, dentists, and other health care practitioners.[29] Federal regulations not only require that certain entities *file* reports with this data bank but also create powerful incentives for hospitals to *request* information from it as part of granting clinical privileges and appointments to their staff.[30] The existence of this data bank and of the information processing provisions of Medicare and Medicaid show that the government is already actively scrutinizing the practice of medicine through reference to and control of personal data.

Private entities have also adopted the model of control through information processing; like the government, they apply personal information technology to strengthen administrative control. Among the private organizations that rely on data processing are insurance companies and other third-party payors, including companies that provide medical insurance through self-insurance, and health maintenance organizations, which are managed care plans that provide comprehensive care services to their enrolled population for a fixed annual payment per enrollee.[31] Government and the private sector

---

Statement of Leslie G. Aronovitz, General Accounting Office, *Medicare/Medicaid Data Bank Unlikely to Increase Collections From Other Insurers*, Before the Committee on Gevernmental Affairs, United States Senate, May 6, 1994.

The Medicare/Medicaid data bank, which is te be established by February 1995, has been unpopular with employers, who have objected to the added paporwork burden that it will impose on them, and with certain government officials, who perceive it leading to scant or no savings. See id. at 1. See also Statoment of Senater Joe Lieberman, Before the Committee on Governmental Affairs, United States Senate, May 6, 1994.

28. 42 U.S.C. §§ 11101-11152 (1988 & Supp. 1993).

29. Id. at § 11101; 45 C.F.R. 60.1-60.14 (1994).

30. The critical language is found in the regulations at 45 C.F.R. 60.10-11 (1994). These sections require hospitals to file requests for information with the National Practitioner Data Bank at certain stated intervals, creato a presumption of knowledge of information in the Data Bank on the part of any hospital that fails to comply with this requirement, and allow disclosure of information in the data bank to medical malpractice plaintiffs *only* when a "hospital failed to request information from the Data Bank as required." 45 C.F.R. 60.11 (a)(5) (1994).

In a similar development concerning attorneys, the American Bar Association has established a data bank of lawyers who have been subject to disciplinary actions. Amy Stevens, *A List of Bad Lawyers to Go On-Line*, Wall St. J. B1 (Aug. 26, 1994). At present, this on-line service is available only to state disciplinary authorities. Id.

31. In the official terminology, the health maintenance erganization ("HMO") provides health care services for a "prepaid capitated rate." Ray and Smith, 42 Drake L. Rev. at 719-20 (cited in note 12). A proposed variation of the HMO that is popular among some policymakers is the organized delivery system. The organized delivery system is a vertically integrated system with physician and health care provider ownership. Id. at 720.

now share many of the same techniques and technology; the state's implementation of DRGs has encouraged the use of similar kinds of price controls by insurance companies and other third-party payors.[32] These private companies can be even more aggressive than the government in their review of personal information when deciding reasonable and customary fees for physicians' services and procedures.[33] In addition, when collecting data about their employees, some private companies go beyond any measures taken by the state regarding its public servants. Many private companies have collected highly sensitive information as part of Employee Assistance Programs, or EAPs.[34] These "wellness programs," which cover almost half of all full-time workers in the United States, seek to improve the health of employees by encouraging them to obtain counseling for psychological problems, stress, and other difficulties. In this fashion, the EAPs lead to the collection of tremendous amounts of highly sensitive information by employers—with the result often being unexpected intrusions into privacy.[35]

The processing and use of health care information by the government and in the private sector already play a critical role in the provision of medical services. Yet, this role will likely be even greater in the future. For example, the Clinton Administration's Health Security Act looked to telecommunications and information technology to reduce costs and improve the delivery of medical care.[36] A key part of this proposal was the assignment of a health security card to all Americans.[37] The Draft Report of the President's Health Security Plan explained that "[m]uch like ATM cards, the health security card allows access to information about health coverage through an integrated national network."[38] This national network of health care information would take the form of a series of linked, regional computer networks. In this system, personal information

---

32. See generally Frolik and Barnes, *Elderlaw* at 408 (cited in note 22); Hall, 137 U. Pa. L. Rev. at 448-57 (cited in note 20).

33. See Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information* 23-37 (1993) ("*Protecting Privacy in Information*").

34. For a discussion of these plans and their weaknesses regarding confidentiality, see Ellen E. Schultz, *Open Secrets: Medical Data Gathered by Firms Can Prove Less Than Confidential*, Wall St. J. A1 (May 18, 1994); *Who's Reading Your Medical Records*, Consumer Reports 628, 632 (Oct. 1994); Joan Hamilton, *Can Company Counselors Help You Cope?*, Business Week 140, 141 (Nov. 14, 1994).

35. See, for example, Hamilton, Business Week at 141 (stating that "EAP data sometimes fall into the wrong hands"). See also notes 79-82 and accompanying text.

36. Health Security Act § 5101 (cited in noto 11).

37. Id. at § 5105.

38. *The President's Health Security Plan: The Draft Report* 124 (Sept. 7, 1993) ("*The Draft Report*").

would be tied to the individual by the assignment of "unique identification numbers for consumers in health plans."[39]

The goal of increasing reliance on data processing technology in the provision of medical care is not unique to the Clinton Administration's plan for health care reform. The Institute of Medicine's Committee on Regional Health Data Networks has recently advocated a similar approach. This group envisions "health database organizations" playing a critical role in the future delivery of medical services.[40] These entities will "have access to (and possibly control of) databases" and a primary mission to publicly release data and the results of analyses done on the databases under their control.[41] To speed the creation of health database organizations and improve the accuracy of their data, the committee advocates a decentralized effort to create computer-based patient records.[42] Along similar lines, the American Hospital Association has called for the establishment of an electronic "health information infrastructure" to which all participants in the healthcare system would be linked.[43]

Information technology may offer the last best hope to control health care costs. It renders accessible to external observation and supervision the enormous amount of data involved in diagnosing, treating, and billing patients. The potential cost savings from greater use of data processing in health care are enormous. In 1993, the Workgroup for Electronic Data Interchange, a voluntary task force comprised of members from the public and private sectors, estimated that switching to a system of electronic data exchange would result in cumulative savings in health care services of forty-two billion dollars by the end of this century.[44]

Information technology is also capable of improving the quality of medical care. As Paul Starr, a sociologist who has advised the Clinton Administration on health care, writes, "The application of information technology to health care holds enormous promise not just to cut the cost of administrative transactions and eliminate duplicate testing, but to reduce errors in treatment and enable profes-

---

39. Id. at 133; Health Security Act § 5104 (cited in note 11).

40. Molla S. Donaldson and Kathleen N. Lohr, eds., *Health Data in the Information Age* 40-90 (National Academy Press, 1994) ("*Institute of Medicine Study*").

41. Id. at 54.

42. Id. at 7.

43. Testimony of the American Hospital Association before the Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations of the United States House of Representatives 2 (May 4, 1994) (copy on file with the Author).

44. Workgroup for Electronic Data Interchange, *1993 Report* iii (Oct. 1993).

sionals and patients alike to make better decisions."[45] The Clinton Administration's health care proposal encouraged the application of information technology to develop treatment protocols and other medical guidelines.[46] Yet, this focus on the practice and regulation of medicine through the processing of personal health care information has a number of potential shortcomings. One of the most important of these drawbacks is the threat to patient privacy.[47]

b. Privacy Concerns

Privacy is, of course, a concept that encompasses a wide variety of interests in American law. The critical privacy interest at stake here is "informational autonomy." The law has long recognized and safeguarded another aspect of self-determination in health care—informed consent in medical decision making. The traditional doctrine of informed consent protects a patient's interest in personal autonomy by requiring doctors and patients to discuss relevant concerns and exchange necessary information before agreeing upon a course of medical treatment.[48]

Like informed consent, informational autonomy relates to the patient's interest in decision making. Autonomous behavior depends on an individual's ability to engage in critical reflection, which forms an essential basis for choices about participation in social and politi-

45. Starr, *The Logic of Health Care Reform* at 93 (cited in note 11). Starr adds, "The greater use of electronic information systems will also help reduce the 'cost of quality' by permitting less burdensome tracking of treatments and outcomes." Id. at 93-94. See Milt Freudenheim, *Health Industry is Changing Itself Ahead of Reform*, N.Y. Times A1, D4 (June 27, 1994) (stating that "[f]or the patient, care could improve as the growing medical networks invest in sophisticated computerized systems that analyze the care received by their many thousands of patients and find ways to improve it").

46. The Health Security Act first required the National Quality Management Council to develop "clinically relevant guidelines" for use by health care providers. Health Security Act § 5006 (a)(1) (cited in note 11). These guidelines were to be presented in different "forms" and "formats." Id. at § 5006 (a)(2)(B)&(C).

In its tort reform section, the act then required the Secretary of Health and Human Services to establish a pilot program "to determine the effect of applying practice guidelines in the resolution of medical malpractice liability actions." Id. at § 5312.

47. Another shortcoming is that application of data processing in medicine may discourage communication with the patient and encourage cookbook medicine, see Paul M. Ellwood, *Shattuck Lecture—Outcomes Management*, 318 New Eng. J. Med. 1549, 1553 (1988).

48. See, for example, *Moore v. Regents of University of California*, 51 Cal. 3d 120, 793 P.2d 479, 483 (1990); *Pratt by Pratt v. University of Minnesota Affiliated Hospitals & Clinics*, 414 N.W.2d 399, 402 (Minn. 1987); *Canterbury v. Spence*, 464 F.2d 772, 783 (D.C. Cir. 1972); *Schloendorff v. Society of New York Hospital*, 211 N.Y. 125, 105 N.E. 92, 93 (1914). The doctrine is, however, far from uncontroversial or even settled, see notes 235-39 and accompanying text.

cal life.[49] Yet, the computer creates a strong pressure for individuals to conform to digital reality.[50] Indeed, even without the use of computers, the collection of information can weaken an individual's capacity for critical reflection and limit the terms upon which she joins in communal life. As history has shown, the collection of information can have a negative effect on the human ability to make free choices about personal and political self-governance.

Totalitarian regimes have already demonstrated how individuals can be rendered helpless by uncertainty about official use of personal information.[51] Risks to individual autonomy even arise in a democratic country, such as the United States, when the law does not put in place adequate legal protections for personal information.[52] Government must protect the capacity of individuals to engage in deliberation about important issues in the conduct of their lives.[53] This notion of "deliberative autonomy" requires legal attention to societal data use and applications. Due to the potential coercive effect of information processing, data protection is a critical precondition to an individual's ability to act as an independent moral agent.

Data protection is of particular importance in the context of personal medical information. Misuse of this information can have an especially negative impact on personal self-government. Consider two examples: Daniel Ellsberg and Michael Eisner. When the Nixon Administration sought to harm Ellsberg, who had leaked the Pentagon Papers to newspapers throughout the United States, the

---

49. For a classic discussion of the connection between human autonomy, critical reflection, and the survival of a democratic order see John Stuart Mill, *On Liberty* ch. 3 (Penguin, 1978) (original ed. 1859). For a thoughtful discussion of the importance of these values within the American democratic tradition, see James E. Fleming, *Constructing the Substantive Constitution*, 72 Texas L. Rev. 211, 253-55 (1993). See also Jed Rubenfeld, *The Right of Privacy*, 102 Harv. L. Rev. 737, 793-94 (1989) (discussing the way state proscription of certain behavior can take over or occupy the totality of a citizen's life).

50. For a discussion of this point, see Schwartz, 43 Hastings L. J. at 1334-43, 1349-52 (cited in note 8).

51. The opening of archives in the former German Democratic Republic has made available a particularly rich body of material on the information gathering of a totalitarian regime. The East German secret police, the Staatssicherheitsdienst, or Stasi, created a dense network of full and part-time spies. The Stasi's goal was the constant observation of the population of East Germany and the resulting promotion of a sense of danger in all human relations. See generally Joachim Gauck, *Die Stasi Akten* (Rowholt, 1991); David Gill and Ulrich Schrötter, *Das Ministerium für Staatssicherheit* 90-97 (Rowohlt Berlin, 1991).

52. Perhaps the clearest example of this risk arose during the McCarthy era. During this time, the Federal Bureau of Investigation set up a large informer network and fed the resulting information about suspected radicals, generally without legal controls, to loyalty boards, employers, and neighbors. See David Caute, *The Great Fear: The Anti-Communist Purge Under Truman and Eisenhower* 111-38 (Simon & Schuster, 1978).

53. John Rawls, *Political Liberalism* 214-35 (Columbia U., 1993); Fleming, 72 Texas L. Rev. at 253-55 (cited in note 49).

cornerstone of its strategy was to gain access to certain of his medical records.[54] This strategy led to a break-in at the office of Ellsberg's psychiatrist, which, characteristically, the responsible henchmen bungled.[55] The goal of Nixon's operatives was to destroy Ellsberg's public image and credibility and to discourage his continuing involvement in political affairs.[56] The Ellsberg case demonstrates that the realms of political self-governance and personal self-governance are complementary:[57] Unauthorized access to Ellsberg's records would have affected both his involvement in the democratic order and his personal autonomy.

The second example concerns Michael Eisner, chairman and chief executive officer of the Walt Disney Company. He is one of the most important and powerful corporate officers in the United States. In addition to his generous salary and stock benefits, Eisner receives extra health benefits as a top Disney executive.[58] Yet, when Eisner was recently stricken with pains in his arms while at a conference of top corporate leaders, he had serious doubts about whether he should submit the resulting bill for medical services to his company's insurance program.[59] According to one report, "Eisner's concern was keeping his health from becoming a topic of conversation at Disney."[60] When Eisner returned to Los Angeles, he went directly to a hospital and underwent emergency quadruple-bypass surgery—but not before taking the precaution of registering at the medical center under an assumed name.[61]

Eisner's concern over his medical records does not have much to do with political self-governance. It has everything to do with his worries about his control over the Disney Company at a time of turmoil in the top executive ranks.[62] This case illustrates the adage that

---

54. *United States v. Liddy*, 542 F.2d 76, 78-79 (D.C. Cir. 1976); Fred Emery, *Watergate: The Corruption of American Politics and the Fall of Richard Nixon* 58-70 (Times Books, 1994).

55. *Liddy*, 542 F.2d at 78-79; Emery, *Watergate* at 67-69.

56. In his memoirs, Richard Nixon candidly admits his "sense of urgency about discrediting what Ellsberg had done and finding out what he might do next." Richard Nixon, *Memoirs* 534 (Grosset & Dunlap, 1984). As far as whether he gave his direct approval for the break-in at Ellsberg's psychiatrist, Nixon first states that he does not believe that he knew of this action before it took place and then adds, in a classic Nixonian construction, "[g]iven the temper of those times and the peril I perceived, I cannot say that had I heen informed of it beforehand, I wonld have automatically considered it unprecedented, unwarranted or unthinkable." Id.

57. Fleming, 72 Texas L. Rev. at 254 n. 211 (cited in note 49).

58. George Anders, *Employee Health Benefits May be Fine, But Look at What Some Executives Get*, Wall St. J. B1, B11 (Oct. 25, 1994).

59. Kim Masters, *A Mouse Divided*, Vanity Fair 166 (Oct. 1994).

60. Id.

61. Id.

62. Id. at 166-72.

knowledge is power: From the lowliest worker anywhere to the mightiest executive at the Magic Kingdom, access to medical information can affect social and economic status and how one leads her life. This example also suggests that one popular aspect of health care reform—its emphasis on preventative medicine—requires safeguards on access to medical data. Preventative medicine requires that people see their health care provider early and often.[63] Yet, without adequate limitations on the dissemination of medical data, individuals will think twice about visits to physicians for anything less than emergencies.[64]

Rather than creating an absolute individual power over personal information, the law should evaluate competing values and strike a balance between individual and societal interests. An individual's control over medical and other personal information cannot be complete because, at least to some extent, these data reflect an outside social reality. Thus, the protection of informational autonomy requires the law to create "fair information practices" that are consistent with and promote an individual's capacity for decision making while also safeguarding society's interest in increasing the efficiency and quality of health service. The creation of fair information practices will be discussed at greater length in this Article's Part IV.

Although the law in this country occasionally recognizes the importance of informational self-determination, it fails to protect this value in the contoxt of health care. It does not put in place the necessary fair information practices. The regulation of the processing of medical data falls far short of creating an effective law of data protection, as is shown by examples provided in the next Part.

---

63. The Clinton Administration's health care proposal stressed the importance of preventative medicine, see Health Security Act § 3331-3334 (cited in note 11) (calling for national initiatives regarding health promotion and disease prevention). See also Eckholm, ed., *Solving America's Health-Care Crisis* at 195 (cited in note 15) (discussing importance of preventative medicine).

64. Indeed, Consumer Union, an influential non-profit organization, is already warning individuals to be careful about the information that they share with their health care provider because of privacy concerns. This organization's advice: "While you should certainly tell your physician everything necessary for proper medical treatment, think twice before disclosing information that has no bearing on your health." *Who's Reading Your Medical Records?*, Consumer Reports at 629 (cited in note 34).

This advice ignores the difficulty of knowing which personal information may be relevant to diagnosis or treatment. Compare *United States v. Westinghouse Electric Corporation*, 638 F.2d 570, 574-80 (3d Cir. 1980) (holding that significant public interest in research designed to improve occupational safety and health permits National Institute of Occupational Safety and Health investigators to view workers' entire medical files because a "heretofore unsuspected" factor may be revealed by such searching examination).

B. Current Data Protection Measures

At present, protection of medical information in this country is less than satisfactory.[65] The regulatory scheme consists of federal law that applies only to data in the control of the government and to certain specific kinds of health information. The scheme also includes various state measures that, taken together, create at best a patchwork of insufficient protection. Moreover, the laws of the various states are far from uniform. In an age of prevalent interstate data transfers, this lack of uniformity is itself an additional weakness in medical data protection in the United States.

The weakness of the regulation of health care information has been commented upon by many observers. The federal Privacy Protection Study Commission in 1977 noted that the billions of visits that Americans make to physicians in a single year and the long period of retention for medical records result in an enormous number of such records in the United States.[66] Yet, this blue-ribbon panel concluded, "even more staggering is the realization of how many people besides the medical-care providers who create a medical record have access to it. . . ."[67] The commission identified numerous flaws in the protection of health care data privacy in the United States. Improvements in this area of law were viewed as a matter of some urgency as "there appears to be no natural limit to the potential uses of medical-record information for purposes quite different from those for which it was originally collected."[68]

The legal scheme has not notably improved since the Privacy Protection Study Commission completed its work almost two decades ago. A recent report by Congress' Office of Technology Assessment concludes, "The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment."[69] According to the Committee on Regional Health Data Networks of the Institute of Medicine, the "threats and potential harm" from disclosure of health records "are real and not numerically trivial."[70] Finally,

---

65. More satisfactory protection is provided for individuals who receive care from federally financed drug and alcohol treatment centers. See notes 124-29 and accompanying text.

66. Privacy Protection Study Commission, *Personal Privacy in an Information Society* 277 (GAO, 1977).

67. Id.

68. Id. at 290-91.

69. Office of Technology Assessment, *Protecting Privacy in Information* at 13 (cited in note 33).

70. *Institute of Medicine Study* at 156 (cited in note 40).

Sheri Alpert, a government policy analyst, notes that "video rental records are afforded more federal protection than are medical records."[71]

The law must contend today with an enormous—and ever growing—demand for personal medical information. This great interest in medical information has not been met by legal regulation that achieves an adequate balance among competing interests. The existing patchwork of laws fails in a number of ways. One shortcoming is the abuse of the notion of "informed consent" to information disclosure.

As has been noted above, informed consent is required to protect not only physical self-determination but also informational self-determination. Consent to the use of one's medical data can only be informed if it follows a genuine disclosure of the intended uses of the personal information. Yet, in the United States, the current norm is "uninformed consent" to disclosure of personal medical data. Service payors, such as insurance companies, and service providers, such as doctors and clinics, generally have their customers, the consumers of health care services, sign "blanket" disclosure releases.[72] These broad disclosure documents have been used to justify almost any secondary use of medical data. Blanket releases have permitted the disclosure of medical information to such bodies as pharmaceutical companies, employers, workers, direct market mailers, and the Medical Information Bureau, a nonprofit association that supplies insurance companies with medical information in order to prevent fraud.[73]

Other kinds of information sharing now take place as a result of vertical integration in the health care sector. Here, no disclosure releases are sought from patients; rather, a company that seeks personal medical information simply buys or merges with the company that has first collected the data. This trend began last year with the merger between Merck & Co., the world's largest pharmaceutical company, and Medco Containment Services, this nation's largest mail

---

71. Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy and Health Care Reform*, 23 Hastings Center Report 13 (Nov.-Dec. 1993). See Joel R. Reidenberg, *Privacy in the Information Economy*, 44 Fed. Comm. L. J. 195, 227-34 (1992) (discussing statutory protection of personal information).

72. Alpert, 23 Hastings Center Report at 13-14.

73. Id. at 15-16; Larry Tye, *List Makers Draw a Bead on Many*, Boston Globe 12 (Sept. 6, 1993); Ray Schultz, *Carlson, Metromail Offer Medical Data*, Direct Marketing News 2 (June 21, 1993); Jerrold Ballinger, *Kmart to Enter Interactive Field with Pharmaceutical Service Line*, Direct Marketing News 1 (Oct. 25, 1993); Office of Technology Assessment, *Protecting Privacy in Information* at 32-35 (cited in note 33).

order pharmacy.[74] Merck, which sought this merger to gain access to Medco's detailed collection of personal medical data, is already making diligent use of this information in marketing its products.[75] Merck's term for this resulting integration of "payors, patients, doctors, pharmacists, other health care providers, and pharmaceutical companies" is "Coordinated Pharmaceutical Care."[76] To carry out similar operations, other drug companies have purchased or are seeking alliances with large pharmacies.[77] According to the *Wall Street Journal*, such drug companies use personal medical information collected by pharmacies "to intervene in relationships among physicians, patients and pharmacists to influence drug selection and use."[78]

Another kind of information sharing takes place within companies that use data generated within Employee Assistance Programs ("EAPs") and employer-managed plans of health insurance. EAPs are employer-sponsored "wellness programs."[79] Workers are encouraged to participate in them for such reasons as reducing stress or obtaining help for family difficulties. Yet, the resulting collections of personal data are increasingly utilized for other purposes, including fighting workers' compensation claims, shifting health care costs to employees with unhealthy lifestyles, and avoiding "litigation from employees soon to be fired or laid off."[80] These uses of personal data currently take place without notice to or consent from employees. Indeed, workers are usually told that their contacts with counselors and psychotherapists will be confidential.[81] Applicable standards of professional ethics, though possibly violated, have not played an im-

74. Joseph Weber, *Is this Rx Too Costly for Merck?*, Business Week 28 (Aug. 9, 1993); Merck & Co., *Interim Report For the Period Ended June 30, 1993* 2-4 (1993) (copy on file with the Author).

75. Elyse Tanouye, *Changing Minds: Owning Medco, Merck Takes Drug Marketing the Next Logical Step*, Wall St. J. A1 (May 31, 1994).

76. Id.

77. A front page story in the Wall Street Journal reported: "SmithKline Beecham PLC recently announced that it will buy United HealthCare Corp.'s Diversified Pharmaceutical Services for $2.3 billion. Pfizer Inc. plans to form close relationships with Value Health Inc. and Caremark International Inc. through strategic alliances." Tanouye, Wall St. J. at A1 (cited in note 75). In addition, Glaxo Holdings, the world's second-largest drug maker, has held talks about an alliance with McKesson Corp.'s PCS Health Systems Inc., which is the largest drug-benefits manager in the United States. Stephen D. Moore, *Glaxo Chairman to Step Down in November*, Wall St. J. A4 (June 16, 1994).

78. Tanouye, Wall St. J. at A1.

79. Schultz, Wall St. J. at A1 (cited in note 34).

80. Id. at A6. See Joan O'C. Hamilton and Michele Galen, *A Furor Over Mental Health*, Business Week 66, 68 (Aug. 8, 1994) (stating that EAPs "can be exploited by companies").

81. Schultz, Wall St. J. at A1 (cited in note 34).

portant role in shaping the behavior of health care providers in this context.[82]

Significant information sharing also occurs within many enterprises that are self-insured.[83] Some companies have even opened their own health clinics for their employees, retirees, and their families.[84] In fact, John Deere & Company, the world's leading manufacturer of farm equipment, recently announced a plan to expand its chain of clinics for its workers in order to supply health care services to other companies' employees.[85] As is the case with wellness programs, personal data have been used in these company-owned health facilities for purposes beyond the actual provision of medical care. For example, worker health care information is used to determine the individual worker's health insurance cost, the extent of covered services, and the worker's continuing employment prospects.[86]

This use of health data could be detrimental not only to the individual worker, but also to the overall efficiency of the labor market in the United States.[87] The distinguished health economist Victor R. Fuchs has noted that employment-based health insurance can harm labor market efficiency. Health insurance in the United States is generally tied to employment; the cost of this insurance represents an ever greater percentage of total compensation; and insurance premiums are now increasingly based on firm-specific-considerations rather than community ratings.[88] These three aspects of the current provision of health insurance have caused more and more decisions about employment and promotion to be based on health-care costs. An employer's decisions about whom to hire, train, and promote, and an employee's choices regarding employment will often depend on the cost and availability of health insurance. Compared to a system of equitable sharing of medical costs throughout the population, this approach introduces significant distortions into the efficiency of the labor market.[89]

---

82. These codes have been criticized as failing to offer meaningful guidance to health care professions and as being widely ignored by them. See Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. Rev. 255, 274-78 (1984).

83. Ellen E. Schultz, *Advantages of Employer Health Plans Are Disappearing*, Wall St. J. C1 (June 17, 1994).

84. Barnaby J. Feder, *Deere Sees a Future in Health Care*, N.Y. Times D1 (July 1, 1994).

85. Id.

86. Fuchs, *The Future of Health Policy* at 12 (cited in note 13).

87. See id.

88. See id.

89. Id. at 12-13.

Thus, the commercial value of personal medical information has led numerous bodies to seek health care information and to use these data for purposes that were not disclosed at the time they were collected. The value of personal medical information has also led to the compilation and sale of lists of persons with specific conditions or diseases. These lists, which detail an individual's most sensitive medical information, are freely trafficked in the United States. For example, Johnson & Johnson has marketed a list of five million elderly incontinent American women.[90] Other companies have advertised lists containing the names of six million allergy sufferers, 700,000 people with bleeding gums, and 67,000 people with epilepsy.[91] Other names appear on a mailing list as suitable consumers of products intended for impotent middle-aged men.[92]

How did we get into the situation in which medical information is so poorly regulated that such lists are offered for sale? Understanding the current regulation's inadequacy requires consideration of how the existing patchwork of laws fails to control the application and use of personal medical data. The regulatory failure occurs in both federal and state law.

1. Federal Measures

At the federal level, data protection measures are found in constitutional law, the Privacy Act, and a few statutes that regulate narrow areas of data use. Any discussion of these provisions must begin by noting their extremely limited coverage. First, the rights contained in the United States Constitution generally protect the individual only from action by the government and not by individuals or groups within the private sector.[93] This limitation is expressed in the "state action" doctrine, which requires either action by the government itself or a close nexus between the government and the

90. Tye, Boston Globe at 12 (cited in note 73). Johnson & Johnson has recently taken this list off the market "in response to privacy concerns." See *Who's Reading Your Medical Records*, Consumer Reports at 629 (cited in note 34).

91. Tye, Boston Globe at 12.

92. *Just Lists Offers "Male Potency" File*, Direct Marketing News 37 (April 19, 1993).

93. See *Georgia v. McCollum*, 112 S. Ct. 2348, 2354 (1992); *Edmonson v. Leesville Concrete Co.*, 500 U.S. 614, 619 (1991); *DeShancy v. Winnebago County Dept. Of Social Services*, 489 U.S. 189, 195-97 (1989). See generally Laurence H. Tribe, *American Constitutional Law* 1688-1720 (Foundation, 2d ed. 1988).

The Thirteenth Amendment, which prohibits slavery, does, of course, apply to private action.

private entity that has infringed a right.[94] Yet, the overwhelming majority of medical information in the United States is not in the hands of the government, but instead is possessed by private doctors, hospitals, and insurance companies. These parties are unlikely to meet the applicable tests for state action, and thus can use information without constitutional restraints.

A second measure of possible value is the Privacy Act, which sets rules only for that data controlled by federal agencies.[95] As a result of this limitation, however, it applies to very little of the total health care information collected. In the 1980s, one expert estimated that this statute applied merely to five percent of the medical data banks in the United States.[96] The other federal statutes that regulate medical data processing focus on even narrower sectors of information use. As a result, most medical data is entirely outside the protections of either constitutional or federal statutory measures. In addition, there are notable weaknesses in each of these federal measures even within their fields of limited application.

When the government collects personal data, a constitutional right to informational privacy applies. Indeed, this right was first identified in a case, *Whalen v. Roe*,[97] that involved medical data. *Whalen* concerned New York State's plan to collect and store information relating to the prescription of certain drugs that had both legitimate and illegitimate applications.[98] These drugs were classified into different schedules, and New York required that prescriptions for certain substances be prepared by a physician in triplicate on an official form. One copy of this form was to be forwarded to the New York State Department of Health in Albany.[99]

In judging the constitutionality of this state scheme, the Supreme Court found that the United States Constitution included a

---

94. The "state action" doctrine is discussed in *McCollum*, 112 S. Ct. at 2354-55; *DeShaney*, 489 U.S. at 195-98. For scholarly criticism of this doctrine, see, for example, Steven J. Heyman, *The First Duty of Government: Protection, Liberty and the Fourteenth Amendment*, 41 Duke L. J. 507, 509 (1992); David A. Strauss, *Due Process, Government Inaction, and Private Wrongs*, 1989 Sup. Ct. Rev. 53, 59.

95. 5 U.S.C. § 552a (1988). The Privacy Act applies only to agencies as defined at 5 U.S.C. § 552(f) (1988). This statute defines agencies as "executive branch" agencies, the "independent" regulatory agencies, and government and government-controlled corporations. Id. The Privacy Act does not, however, extend to records of Congress. It also does not apply to federal courts or state and local governments.

96. Terra Ziporyn, *Hippocrates Meets the Data Banks*, 252 J.A.M.A. 317, 318 (July 20, 1984) (quoting Professor Vincent M. Brannigan).

97. 429 U.S. 589 (1977).

98. Id. at 591.

99. Id. At 592-93.

right of informational privacy that prohibited "disclosure of personal matters" and protected "independence" in decision making.[100] The nondisclosure interest was supported by reference to cases grounded in the First and Fourth amendments.[101] The second interest, that of independence in decision making, rested on the protection of certain intimate activities under substantive due process.[102]

The Supreme Court decided that New York's plan for data collection did not impinge upon these two interests. The first interest—avoiding disclosure of personal matters—protects against public disclosure of information surrendered to the government.[103] To check whether the nondisclosure interest had been violated, the Court examined the data security measures of New York. These measures included storing the prescription forms in a vault until their ultimate destruction; surrounding the room in which these data were received with a wire fence and protecting this area with an alarm system; and promulgating statutory and regulatory measures that prohibited disclosure to the public.[104] The Court found such actions were well designed to insure that the personal medical data collected by the state government would be kept from the public.[105]

The second *Whalen* interest—independence in making certain types of important decisions—was implicated by the patient's decision whether to acquire and use needed medicine.[106] The Court found that New York's data processing scheme did not violate this interest. Although the government's record-keeping had discouraged some use of the drugs in question, "the decision to prescribe, or to use" remained in the control of the physician and the patient.[107] While open to criticism for certain doctrinal weaknesses,[108] the *Whalen* two-branch approach offers a model with considerable potential for the

100. Id. at 598-600. The Court was less than precise about the exact constitutional basis of this right. In a footnote, it cites prior opinions, *Roe v. Wade*, 410 U.S. 113, 152 (1973) and *Palko v. Connecticut*, 302 U.S. 319, 325 (1937), for the proposition that the basis of this right is the Fourteenth Amendment's concept of personal liberty. 429 U.S. at 598-99 n. 23. Yet, the Court also cites elsewhere to other constitutional provisions, see notes 101-02 and accompanying text.

101. 429 U.S. at 599 n.25.

102. Id. at 600 n. 26. For an analysis of the difficulties and the promise of this approach, see Paul M. Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 Am. J. Comp. L. 675, 677-86 (1989).

103. 429 U.S. at 599-602.

104. Id. at 593-94.

105. Id. at 601-04.

106. Id. at 603.

107. Id.

108. Schwartz, 37 Am. J. Comp. L. at 677-85 (cited in note 102). These weaknesses relate to two other kinds of privacy law: sexual privacy and Fourth Amendment privacy. Id.

protection of informational self-determination. Lower courts have not, however, successfully developed this potential.

Lower courts analyzing governmental attempts to obtain or examine medical information have done so primarily with reference to the first *Whalen* interest, that of nondisclosure.[109] Unfortunately, these courts have analyzed this interest in an inconsistent fashion. Some lower courts have found that this interest in nondisclosure applies only to a narrow group of fundamental constitutional rights.[110] Indeed, some courts have even viewed *Whalen* as a decision that sanctions all "legitimate" governmental requests for medical data.[111] And, the autonomy interest identified in *Whalen* has been almost entirely absent from case law.[112] Thus, although *Whalen* offers a potentially useful element in the overall structure of an American data protection law, it has not led to vigorous protection of medical privacy.

Federal statutory measures have not adequately supplemented the limited constitutional protection for medical privacy. As stated before, the Privacy Act applies only to medical records in the control of federal agencies,[113] and even this limited coverage is not without

---

109. See, for example, *American Civil Liberties Union v. Mississippi*, 911 F.2d 1066, 1069-70 (5th Cir. 1990); *Doe v. Attorney General*, 941 F.2d 780, 795 (9th Cir. 1991); *Mann v. University of Cincinnati*, 824 F. Supp. 1190, 1198-99 (S.D. Ohio 1993); *Doe v. Borough of Barrington*, 729 F. Supp. 376, 382 (D. N.J. 1990); *Soucie v. County of Monroe*, 736 F. Supp. 33, 35-37 (W.D. N.Y. 1990).

110. See, for example, *Walls v. City of Petersburg*, 895 F.2d 188, 192-94 (4th Cir. 1990) (applying a nondisclosure interest to a right to privacy); *Ramie v. City of Hedwig Village, Texas*, 765 F.2d 490, 492 (5th Cir. 1985) (same).

111. See *Gutierrez v. Lynch*, 826 F.2d 1534, 1539 (6th Cir. 1987) (stating that "legitimate requests for medical information do not constitute an invasion of the right to privacy").

112. Compare *Plante v. Gonzalez*, 575 F.2d 1119, 1128-32 (5th Cir. 1978) with *Mann v. University of Cincinnati*, 824 F. Supp. 1190, 1198-99 (S.D. Ohio 1993).

113. The Privacy Act does not apply to private organizations or to not-for-profit corporations that do bnsiness with the United States government. Even corporations funded and regulated by the federal government are not automatically within the reaches of the Privacy Act. "'[E]xtensive, detailed and virtually day-to-day supervision' by the federal government is needed before 'agency' status [attaches]." *St. Michael's Convalescent Hospital v. California*, 643 F.2d 1369, 1374-79 (9th Cir. 1981) (quoting *Forsham v. Harris*, 445 U.S. 169, 180 (1980)). See also *Unt v. Aerospace Corporation*, 765 F.2d 1440, 1447 (9th Cir. 1985) (refusing to apply the Privacy Act te a nonprofit corporation formed to provide engineering expertise to the Air Force).

Since the Privacy Act applies to the records of federal agencies alone, it does not control records that these agencies seek to obtain from private organizations. This distinction between disclosure from an agency and from a private organization can have importance in the context of health care information. A recent decision of the Fifth Circuit regarding medical records, *Gilbreath v. Guadalupe Hospital Foundation, Inc.*, 5 F.3d 785 (5th Cir. 1993), is illustrative of this point.

In *Gilbreath*, the plaintiff sued to prevent the release of certain hospital records that contained information about the treatment that she and her son received for gunshot wounds at two hospitals. Local newspapers had reported that the plaintiff's husband had shot her and their son; these reports had led to the husband's removal from a job at a federal agency. Id. at 787-88. When the plaintiff's husband contested this dismissal, the Merit Systems Protection

flaws. The most notable shortcoming is in the Privacy Act's insufficient control of secondary use. Although the Privacy Act generally permits the disclosure of records only "pursuant to a written request by, or with the prior written consent of the individual to whom the record pertains,"[114] no fewer than twelve exceptions exist to this requirement.[115] Of these, the most problematic is the "routine use" exception, which has been made into an enormous loophole.[116] Agencies have justified a wide variety of data disclosures as the "routine use" of personal information. For example, the Veterans Administration has created no fewer than thirty-eight "routine" uses, some exceedingly broad, for its patients' medical records.[117]

Provisions of federal law other than the Privacy Act provide some protection for medical records. One such measure provides data protection for the social security records of the Department of Health and Human Services.[118] However, this statute does allow for disclosures both "as otherwise provided by Federal law" and pursuant to regulations issued by the Secretary.[119] In addition, Federal laws which restrict the use of data after it has been obtained have proven

---

Board, an independent, quasi-judicial federal agency that adjudicates appeals by federal employees from adverse personnel actions, sought production of these hospital records. Id. The Gilbreath court found that the Privacy Act did *not* prevent disclosure of these records because the two hospitals whose records were sought were not "agencies" within the meaning of this statute. Id. at 791. It did not matter that the records were sought by a federal agency; the Privacy Act only applies to disclosure *from* agencies, not from private organizations *to* agencies. Id.

114. 5 U.S.C. § 552a(b) (1988).

115. Id. at (b)(1)-(12).

116. Id. at (b)(3). For criticisms of the "routine use" loophole, see Flaherty, *Protecting Privacy* at 323-24 (cited in note 8); Bennett, *Regulating Privacy* at 108-10 (cited in note 8); Tedd Rohert Cole, *Does the Privacy Act of 1974 Protect Your Right of Privacy? An Examination of the Routine Use Exemption*, 40 Am. U. L. Rev. 978, 991 (1991).

117. Privacy Act Issuances, 1991 Comp., Volume 2, 938-41. For example, one "routine" use permits disclosure of records to "Federal, State and local government agencies and national health organizations in order to assist in the development of programs that will be heneficial to claimants and to protect their rights under law and assure that they are receiving all benefits to which they are entitled." Id. at 939. This standard allows the release of personally identifiable information in instances in which aggregate data would suffice.

Another exception allows release to "a member of the general public" who makes "an inquiry about a named individual" regarding "the amount of monthly VA monetary benefits being received hy the patient." Id.

118. 42 U.S.C. § 1305 (1988). Social security records often contain a variety of medical information. This information is most typically collected in connection with claims for disability benefits. See generally Jerry L. Mashaw, *Bureaucratic Justice: Managing Social Security Disability Claims* (Yale U., 1983). A federal statute prevents "any officer or employee of the Department of Health and Human Services in the course of discharging" the social security program from disclosing any "file, record, report or any other paper, or information, obtained at any time by any person" from the Department. 42 U.S.C. § 1306 (1988).

119. 42 U.S.C. § 1306 (1988). The regulations are found at 20 C.F.R. §401.100 et seq. (1994).

ineffective. For example, the Americans with Disabilities Act ("ADA") generally forbids employers from considering an employee's health in making employment decisions.[120] Unfortunately, this protection has proven less than efficacious because job applicants are often either unaware or unable to prove that employers considered their health information.[121] Even less helpful is the Age Discrimination in Employment Act ("ADEA"),[122] which prohibits hiring or firing decisions based on age but not on health factors.[123]

Federal law also safeguards the data of patients who undergo treatment for alcohol or drug abuse in programs receiving federal funds or subject to federal regulation.[124] These laws strive to ensure confidentiality in order to encourage participation in alcohol and drug treatment programs.[125] As a result of these generally effective laws, the best data protection for health information in the United States is provided for patients who receive treatment for substance abuse in federally-funded clinics.

The success of these federal statutes is grounded in the careful way that they treat the issue of disclosure of patient information. To begin with, they permit disclosure to take place only under certain specified conditions.[126] Moreover, in place of "uninformed consent,"

---

120. 42 U.S.C. § 12101 (Supp. 1993).

121. See generally Robert L. Burgdorf, Jr., *The Americans with Disabilities Act: Analysis and Implications of a Second Generation Civil Rights Statute*, 26 Harv. C.R.-C.L. L. Rev. 413, 434-37 (1991); Scbultz, Wall St. J. at C20 (cited in note 34).

122. 29 U.S.C. § 621 et seq. (1988).

123. 29 U.S.C. §§ 621-634 (1988). As a leading casebook has explained the matter, "The employer . . . may terminate an ADEA covered employee for almost any reason other than age. . . . An employer may fire for declining health, diminished vigor, reduced competence, or even health problems related to advanced age. What the employer may not do is fire *merely* because of the employee's age." Frolik and Barnes, *Elderlaw* at 163 (cited in note 22).

124. 42 U.S.C. §§ 290dd-1 (1988 & Supp. 1994).

125. See *Whyte v. Conn. Mutual Life Ins. Co.*, 818 F.2d 1005, 1010 (1st Cir. 1987) (stating that the relevant "regulations place the confidentiality necessary to ensure the success of alcoholism treatment programs above [the need to use statements made during treatment as evidence], and we must respect that decision"); *Heartview Foundation v. Glaser*, 361 N.W.2d 232, 235 (N.D. 1985) (stating "[w]ithout the assurance of confidentiality a number of individuals may hesitate to seek treatment in alcohol- and drug-treatment programs")

126. The general standard of the law is that patient records are not to be disclosed. 42 U.S.C. § 290dd-2(a) (1988 & Supp. 1994). There are four exceptions to the general standard of nondisclosure: (1) in accordance with the prior written consent of the patient; (2) to medical personnel to the extent necessary to meet a medical emergency; (3) to qualified personnel to conduct scientific research, audits, or program evaluations; and (4) if authorized by court order. 42 U.S.C. § 290dd-2 (1988 & Supp. 1994).

Of the four circumstances in which information pertaining to drug or alcohol abuse treatments may be released, the two most important are court orders and patient consent. As for disclosure pursuant to a ceurt order, the judicial decision whether or not to release patient data is to be made pursuant to a balancing test. The statutory test requires judicial disclosure "after application showing good cause thereof," 42 U.S.C. § 290dd-2(b)(2)(C), and, more specifically,

these laws carefully define the conditions necessary for the patient to give "informed consent" to release data.[127] Written consent to a disclosure must include an explanation of matters such as: (1) the purpose of disclosure; (2) how much and what kind of information is to be disclosed; and (3) a statement that the consent is subject to revocation at any time.[128] Each disclosure must also be accompanied by a written statement that prohibits redisclosure.[129] These statutes not only offer an excellent contrast to the "blanket" consent that frequently is found elsewhere, but also show the potential for the success of additional federal efforts to protect the privacy of medical information.

It should be mentioned again that these federal protections generally apply only to government action. Only in strictly limited circumstances does current federal law protect health care information in the private sector. Thus, private clinics for substance abuse that receive federal money are obliged to follow these federal rules for medical information, but privately funded clinics are not. The regulation of health care information is largely the province of state law.

2. State Measures

Existing state law does not successfully overcome the weaknesses in current federal data protection. Although many different kinds of legal provisions on the state level relate to medical information, these measures do not create an effective system of data protection. First, some state constitutions, most notably California's, have been interpreted as setting limits on the collection and dissemination of medical data.[130] Also, most states recognize that the relationship

---

states, "In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services." Id. This balancing test is developed further by the applicable regulation. 42 C.F.R. 2.61-2.67 (1994).

The statutory balancing test and the regulations have been carefully applied by a number of courts. These courts generally assess the seriousness of any alleged crime to have been committed by the person against whom disclosure is sought and check to see that redisclosure of the information will not occur beyond the immediate application necessary in the case at hand. *Whyte*, 818 F.2d at 1009-12; *State v. Rollinson*, 203 Conn. 641, 526 A.2d 1283, 1291-93 (1987); *Heartview Foundation v. Glaser*, 361 N.W.2d 232, 233-35 (N.D. 1985); *In the Matter of Baby X*, 97 Mich. App. 111, 293 N.W.2d 736, 739-41 (1980); *In the Matter of Dwayne G.*, 97 Misc. 2d 333, 411 N.Y.S.2d 180, 182-84 (Family Ct., Kings County 1978); *United States v. Graham*, 548 F.2d 1302, 1314 (8th Cir. 1977).

127. 42 U.S.C. § 290dd-2 (1988 & Supp. 1994).

128. Id.

129. Id.

130. Cal. Const., Art. I, § 1. For cases construing California's constitutional right to privacy, see, for example, *Urbaniak v. Newton*, 226 Cal. App. 3d 1128, 277 Cal. Rptr. 354, 357-58

between doctor and patient gives rise to a general duty of confidentiality.[131] Some states have extended this duty of confidentiality to hospitals.[132]

State statutes also require that certain reports concerning specific diseases or medical conditions be filed with state health authorities by physicians, hospitals, and laboratories. These reports concern knife and gunshot wounds, sexually transmitted diseases, HIV infection, and communicable diseases such as tuberculosis.[133] Reports must also be filed about injuries to children or elderly individuals that might indicate abuse.[134] Despite the highly sensitive nature of these public health data, state laws often contain neither adequate limitations on the use of the information nor adequate restrictions on the time for which these data will be stored.[135]

Some protection for medical privacy is also offered by common law tort remedies. The common law right of privacy prevents public disclosure of private facts.[136] Most courts have, however, found that such a claim requires widespread disclosure to the public, which will not occur in most cases involving release of medical information.[137] Another restrictive element of the public disclosure tort is that most courts require disclosure to someone without a "legitimate interest" in

---

(1991); *Division of Medical Quality v. Gherardini*, 93 Cal. App. 3d 669, 156 Cal. Rptr. 55, 61-62 (1979).

131. See, for example, Cal. Civil Code § 56 (West 1982); Wisc. Stat. Ann. § 146.82 (West 1989); R. I. Gen. Laws § 5-37-9 (1987). For cases interpreting this duty of confidentiality, see, for example, *Horne v. Patton*, 291 Ala. 701, 287 S.2d 824, 827-30 (1974); *Hague v. Williams*, 37 N.J. 328, 181 A.2d 345, 347-49 (1962).

132. See, for example, Cal. Civil Code § 56.10 (West 1982 & Supp. 1994); Wisc. Stat. Ann. § 146.81 (West 1989 & Supp. 1994).

133. See, for example, Ark. Stat. Ann. §§ 12-12-602 (1987) (reporting of knife and gunshot wounds), 20-16-501 (1987) (reporting of "evidence suggestive of . . . venereal diseases"); Cal. Health & Safety Code § 199.21 (reporting of blood test regarding HIV). See Gellman, 62 N.C. L. Rev. at 274-78 (cited in note 82).

134. See, for example, Ark. Stat. Ann. § 5-28-201 (1987); Ind. Code § 31-6-11-4 (1987); Mich. Comp. Laws § 722.621 et seq. (1993 & Supp. 1994); New York Soc. Serv. Law §§ 411-428 (McKinney 1992).

135. Compare *Valmonte v. Bane*, 18 F.3d 992 (2nd Cir. 1994) (striking down New York system of maintaining data bank of suspected child abusers) with *Arkansas Department of Human Services v. Heath*, 312 Ark. 206, 848 S.W.2d 927 (1993) (upholding Arkansas system of maintaining a child abuse data bank that permits storing of "unsubstantiated reports").

136. See Restatement (Second) of Torts § 652D at 383 (1977); W. Page Keeton, et al., *Prosser and Keeton on the Law of Torts* § 117 at 856-63 (Foundation, 5th ed. 1984).

137. *Porten v. University of San Francisco*, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839, 841 (1976); *Timperley v. Chase Collection Service*, 272 Cal. App. 2d 697, 77 Cal. Rptr. 782, 784 (1969). But see *Miller v. Motorola*, 202 Ill. App. 3d 976, 560 N.E.2d 900, 902 (1990) (holding that required communication must not be to the public at large, and a "special relationship" to the specific "public" to whom the information is disclosed is needed); Keeton, et al., *Prosser and Keeton on Torts* § 117 at 857-58 (criticizing the requirement of public disclosure).

the information.[138] And, some courts consider employers to have such a legitimate interest in much of their workers' medical information.[139]

The tort right of privacy also prevents intentional intrusions upon the private affairs or concerns of an individual.[140] Such intrusions, however, must be "highly offensive."[141] This branch of the tort also requires that "there . . . be something in the nature of prying or intrusion."[142] *Miller v. Motorola*[143] illustrates the weakness of this intrusion tort for protecting medical privacy. In this case, an employer disclosed sensitive medical information to the plaintiff's coworkers.[144] The Illinois court found no "intrusion" on the plaintiff because she had "voluntarily provided" the information to her employer.[145]

Finally, a Uniform Health Care Information Practices Act has been drafted.[146] Only a small number of states, however, have adopted this law.[147] Since the Uniform Act is subject to modification by state legislatures before passage, widespread adoption of this law might not improve the level of protection for health care information.

These provisions have failed to impose a consistent framework on the use of medical information by primary care providers, supporting physicians, health care institutions, and secondary users. This lack of uniformity is even more striking when one compares the legal systems of different states. Yet, flows of health care information now take place on an interstate level. As noted in one recent study:

> A state-by-state approach to regulation of medical information does not reflect the realities of modern healthcare finance and provision. The flow of medical information is rarely restricted to the state in which it is generated. Such information is routinely transmitted to other states, subject to different legal requirements, for a wide variety of purposes ranging from medical consultation and research collaboration to governmental monitoring for quality.[148]

---

138. Keeton, et al., *Prosser and Keeton on Torts* § 117 at 857-58.

139. Id. But see *Horne v. Patton*, 291 Ala. 701, 287 S.2d 824, 829-30 (1973) (holding that a physician may be held liable for disclosing information to an employer).

140. Restatement (Second) of Torts, § 652B at 378 (1977).

141. Id.

142. Keeton, et al., *Prosser and Keeton on Torts* § 117 at 855 (cited in note 136).

143. 202 Ill. App. 3d 976, 560 N.E.2d 900 (1990).

144. Id. at 903.

145. Id.

146. Uniform Health Care Information Act, 9 (Part I) U.L.A. 475 (1985 & Supp. 1994).

147. See Mont. Code Ann. § 50-16-501 (1987); Wash. Rev. Code Ann. § 70.02.005 (West 1991). For a discussion, see Lawrence O. Gostin, et. al., *Privacy and Security of Personal Information in a New Health Care System*, 270 J. A.M.A. 2487, 2490 (1993).

148. Gostin, et al., 270 J.A.M.A. at 2489-90.

Whether as a result of regional health care alliances or an increased reliance on health data base organizations, national health care reform will increase transfers of medical information between different states.

The interstate flow of medical information calls for a federal response to these issues. The response should be embodied in a specific law that regulates the processing of health care data. Professor Spiros Simitis, an international data protection expert, has urged an abandonment of any search for "abstract, generally applicable provisions" in favor of "a context-bound allocation of information embodied in a complex system of both specific and substantive regulations."[149] An essential element of a system of regulation for health care information is the articulation of legally binding fair information practices. These fair information practices must be established now as part of national health care reform—not at some date in the future. In an age of rapid technological change, privacy lost is not frequently regained. Indeed, once unfettered technology has caused social expectations of privacy to sink, the law often chooses simply to sanction this loss.[150]

Data protection must be structured as an essential element of health care reform; fair information practices must be part of the same laws that authorize the collection and retrieval of personal health care data. The Clinton Administration did set up many useful privacy protections in the Health Security Act's Subtitle V. Unfortunately, the act did not provide an entirely adequate structure for fair information practices. The act proposed first the establishment of an electronic data network of health care information followed, some years later, by the creation of "a detailed proposal for privacy protection legislation."[151] The latter scheme, which was to include detailed fair information practices, was to be submitted

149. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. Pa. L. Rev. 707, 742 (1987).

150. The classic example of the law sanctioning the loss of privacy caused by technology occurs when the Supreme Court searches for a "reasonable expectation of privacy" under the Fourth Amendment. Compare *Florida v. Riley*, 488 U.S. 445, 451-52 (1989) (plurality) (stating that helicopters flying at 400 feet are not sufficiently rare in this country to create a reasonable anticipation of not being observed from that altitude) with id. at 456 (Brennan, J., dissenting) (arguing that critical test under Fourth Amendment should be "whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining te citizens would be diminished to a compass inconsistent with the aims of a free and open society") (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 403 (1974)).

151. Health Security Act §§ 5120-5123 (cited in note 11).

within *three years* of the enactment of the Health Security Act.[152] In fairness to the Clinton Administration, it should be stated that it did prove responsive to demands for additional measures regarding health care privacy, supporting an important Congressional effort in this regard.[153] Unfortunately, the resulting bill was not passed by Congress.

Any delay in articulating fair information practices will allow the rules of the road for the use of medical data to be shaped by seemingly inexorable technological imperatives. Instead of an ex post facto approach, privacy protection must be built into any health information network at the time of its construction.[154]

III. INTERNATIONAL DEVELOPMENTS

Developments in Europe provide both an important example of medical privacy protection and an independent additional ground for the passage of a fair information practices act in this country. This Part examines how national and transnational laws regulate the processing of medical data in Europe, and analyzes how the inadequate protection of medical data in the United States will lead to the blocking of personal information transfers into our country and will limit the ability of American companies to process European records.

Within Europe, medical data are subject to a variety of legal measures. As in the United States, data protection in European nations begins with constitutional law. In the Federal Republic of Germany, for example, an important constitutional right applies to all personal information, including medical data.[155] Unlike the United States, however, most European nations have enacted omnibus data

---

152. Id. at § 5122. The most detailed discussion of privacy issues in health care reform by the Clinton Administration can be found in *The Draft Report* at 136-38 (cited in note 38). See also *Health Security Report* at 57 (cited in note 11).

153. The bill in question, the Fair Health Information Practices Act of 1994, is discussed in Part IV.E.

154. The Committee on Regional Health Data Networks of the Institute of Medicine has reached a similar conclusion. This organization not only advocates the enactment of a federal fair information practices law, but urges Congress to act "as soon as possible." *Institute of Medicine Study* at 191 (cited in note 40).

155. This right was first identified in an important decision of the German Constitutional Court, 65 Entscheidungen des Bundesverfassungsgerichts 1 (1983). An English translation of this case with excellent commentary is found in Donald P. Kommers, *The Constitutional Jurisprudence of the Federal Republic of Germany* 332-36 (Duke U., 1989). Since this initial decision, the German High Court has further developed this important right. See, for example, Neue Juristische Wochenschrift ("NJW") 707 (1989), NJW 2805 (1987).

protection laws that regulate both the public and private sectors.[156] These general laws are supplemented and strengthened by other laws that contain more precise regulations for individual areas of processing activities. In Germany, for example, medical data are subject to the Federal Data Protection Law,[157] the Code of Social Law (*Sozialgesetzbuch*),[158] the Criminal Code,[159] the Civil Code,[160] and state data protection laws.[161] The resulting level of data protection for medical information in Europe, although not without flaws, is generally at a far higher level than in the United States.

Some German examples will illustrate this high level of protection and demonstrate the possibility of future difficulties. The Federal Data Protection Law regulates the possibility of transfers of personal information for direct marketing purposes.[162] It generally forbids transfers when the data in question relate to "health"

156. English translations of these laws are found in Spiros Simitis, Ulrich Dammann, and Marita Körner, eds., *Data Protection in the European Union* (Nomos, 1994) ("*Data Protection Statutes*"). See generally Bennett, *Regulating Privacy* at 153-92 (cited in note 8); Flaherty, *Protecting Privacy* at 21-39, 93-101, 165-74 (cited in note 8); Paul M. Schwartz, *Das Übersetzen im Datenschutz: Unterschiede zwischen deutschen und amerikischen Konzepten der „Privatheit,"* 8 Recht der Datenverarbeitung 8 (1992).

157. Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990 (BGBl. I S.2954) ("German Data Protection Law"). An English translation of this law can be found in *Data Protection Statutes*.

158. Sozialgesetzbuch, Zehntes Buch (X), vom 18.August 1980 (BGBl. I S. 1469) ("Code of Social Law"). Critical elements of data protection are found in the fifth and tenth books of the Code of Social Law. Sozialgesetzbuch, Zehntes Buch (X), Fünftes Buch (V). Important changes have been made in both parts of the Social Law, see Zweites Gesetz zur Änderung des Sozialgesetzbuchs vom 13.Juni 1994 (BGBl. I S.1229) (amending the tenth book of the Social Law), Zweites Gesetz zur Änderung des Fünften Buches Sozialgesetzbuch vom 20.12.91, BGBl. I S.2325 (amending the fifth book of the Social Law).

159. Strafgesetzbuch, 203 I, Nr. 3.

160. Bürgerliches Gesetzbuch § 134 ("Civil Code").

161. Among the most interesting state data protection laws are those found in the "new states" (neue Länder), that is, the entities formed out of the former German Democratic Republic. See, for example, Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten (Landesdatenschutzgesetz von Mecklenburg-Vorpommern) (Data Protection Law of Mecklenburg-Vorpommern) in *Data Protection Statutes* (cited in note 156); Gesetz zum der informationellen Selbstbostimmung im Freistaat Sachsen (Data Protection Law of Saxony), in *Data Protection Statutes*.

This special attention of the new German states to the need for informational privacy extends to their constitutional law. Every one of the constitutions promulgated in the new German states contains an explicit right to data protection. See Verfassung des Landes Brandenburg (Constitution of Brandenburg), Art. 11; Verfassung des Landes Mecklenburg-Vorpommern (Constitution of Mecklenburg-Vorpommern), Art. 6; Verfassung des Freistaates Sachsen (Constitution of Saxony), Art. 33; Verfassung des Landes Sachsen-Anhalt (Constitution of Saxony-Anahlt), Art. 6; Verfassung des Freistaat Thüringen (Constitution of Thuringia), Art. 6.

162. German Data Protection Law, § 28(2)(b) (cited in note 157).

(*gesundheitliche Verhältnisse*).[163] The Code of Social Law[164] follows a similar approach. It permits information, including medical data, collected in the administration of social welfare programs to be processed, stored, and transferred only when a specific legal measure permits such action.[165] This law contains no specific provision allowing medical data to be used for direct marketing purposes.[166]

Germany also forbids the transfer of personal patient data to "clearinghouses" (*Verrechnungsstellen*) without patient consent.[167] These services function as "factoring" enterprises; they purchase debts owed physicians for private medical services at a discount and then undertake to collect the amount owed.[168] The Supreme Civil Court found that this practice violated the physician's duty of confidentiality as set out in the Civil Code and Criminal Code.[169] The Court required that patients be informed of the physician's intent to transfer patient data and give their consent in writing.[170]

Health identification cards are an area of future difficulty in Germany. Germany health insurance couples a guarantee of universal access to medical care with global budgetary constraints on physicians and hospitals.[171] Beginning in the late 1980s, this approach to health insurance ceased to contain health care expenditures.[172] A critical part of the legal response to this situation has been the aggressive use of data collection to control patient and physician behavior.[173] The Health Reform Law of 1989 required that all patients be furnished with machine-readable health insurance

---

163. Id. See Herbert Auernhammer, *Bundesdatenschutzgesetz* 375 (Carl Heymann, 3d ed. 1993).

164. Code of Social Law (cited in note 158).

165. Id. at §§ 67-78.

166. Id. at §§ 67c-78.

167. BGH, Judgment of July 10, 1991, NJW 2955 (1991) ("*Supreme Civil Court Decision*").

168. Id. at 2955-56.

169. Id at 2956-57. See Civil Code § 134 (cited in note 160); § 203 I Nr. 1 Strafgesetzbuch (cited in note 159).

170. *Supreme Civil Court Decision* at 2957 (cited in note 167). For a discussion of this important decision, see Marita Körner-Dammann, *Weitergabe von Patientendaten an ärztliche Verrechnungsstellen*, NJW 729 (1992); Herbert Auernhammer, *Zum Honorareinzug durch ärztliche Verrechnungsstellen*, 16 Datenschutz und Datensicherung 182 (1992).

171. For an explanation of Germany's provision of medical services, see generally John K. Iglehart, *Germany's Health Care System*, 324 New Eng. J. Med. 503 (1991) (first of two parts); Uwe E. Reinhardt, *Reforming the Health Care System: The Universal Dilemma*, 19 Am. J. of Law & Med. 21 (1993).

For a discussion of the reform of this system in the 1980s, see John K. Iglehart, *Germany's Health Care System*, 324 New Eng. J. Med. 1750, 1751-55 (1991) (second of two parts); Jan Kuhlmann, *Die Verarbeitung von Patientendaten nach dem SGB V. und das Recht auf selbstbestimmte medizinische Behandlung*, 17 Datenschutz und Datensicherung 198, 199-200 (1993).

172. Kuhlmann, 17 Datenschutz und Datensicherung at 198, 199-200.

173. Id.

cards by the start of 1995.[174] Strict legal limits have been placed on the type of information that can be stored on this card and on the sharing of data generated through its use.[175]

Recently, however, numerous proposals have been made to introduce more technically complex "chip cards."[176] These identification cards contain not a simple magnetic strip, such as that found on most credit cards and the current German health identification card, but a small silicon chip.[177] In pilot programs in Germany, such cards are already being used to store health care information.[178] A "chip card" is already capable of storing the contents of a newspaper; in the future, even greater storage capacity will be possible.[179] One day a patient will be able to carry about her entire medical record on a single plastic card.[180] The data protection issues raised by this technology are only beginning to be explored. Indeed, at present, no social, political, or legal consensus has been reached about the appropriate use of the chip card in the provision of medical services in Germany.[181] Data protection commissioners on the federal and state levels are playing a critical role in leading the public discussion regarding the acceptability of this device.[182]

A European-wide treaty also affects the level of protection for medical information within any European nation. The Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data is a "non-self-executing treaty"; its standards do not impose directly binding norms on signatory nations. It does, however, require signatory nations to establish domestic data protection laws that will give effect to the

---

174. Id. Among the most important uses of the information contained on these cards is placing a global cap on the total cost of medical services that any given physician may furnish. Id. at 204. A physician who exceeds the average costs of services in a given time period by more than twenty percent is to be refused additional insurance compensation for this additional work. Id.

175. Code of Social Law, Book V, §§ 284-305 (cited in note 158).

176. See generally *Die Lunte Brennt*, Der Spiegel 62, 68-72 (47/1994).

177. Id. See Rita Wellbrock, *Chancen und Risiken des Einsatzes maschinenlesbarer Patientenkarten*, 18 Datenschutz und Datensicherung 70 (1994).

178. Der Hessische Datenschutzbeauftragte, 22. *Tätigkeitsbericht* 59-61 (1993) (*"Twenty-Second Activity Report of the Hessian Data Protection Commissioner"*).

179. *Die Lunte Brennt*, Der Spiegel at 66 (cited in note 176).

180. Id. at 78-79; Wellbrock, 18 Datenschutz und Datensicherung at 70 (cited in note 177).

181. *Die Lunte Brennt*, Der Spiegel at 78-79; Wellbrock, 18 Datenschutz und Datensicherung at 74.

182. See Landesbeauftragte für den Datenschutz, Bremen, 16. Jahresbericht 63-66 (1994); Landesdatenschutzbeauftragte für den Datenschutz, Bremen, *Ärztliche Behandlung und Abrechnung der Leistungen demnächst nur noch mit Chipkarte*, 16 Datenschutz und Datensicherung 276 (1992); *Twenty-Second Activity Report of the Hessian Data Protection Commissioner* at 58-93 (cited in note 178).

convention's principles. The convention, the most important existing European agreement for data protection, requires signatory nations to permit the processing of sensitive data, including "personal data concerning health," only when "domestic law provides appropriate safegnards."[183] Such safeguards include rights of access and correction; a specification of collection purposes; data security measures; and limitations on unnecessary data collection and data uses that are incompatible with the original collection purpose.[184] In addition, national laws must provide remedies for lack of compliance with requirements regarding collection of personal data, access to one's personal data, and correction of personal data.[185]

The convention's provisions apply to all processing of personal data. These omnibus protections have been expanded by the Council of Europe's Recommendation No.R(81) 1, which provides narrower regulations for automated medical data banks.[186] These regulations provide additional data protection for collections of health care data. The recommendation's requirements "are to be taken duly into account not only with regard to medical data banks which are operational, but also those which are in the developmental phase."[187] The new Draft Recommendation on the Protection of Medical Data will provide even more detailed, and in many respects stronger, protection for medical data.[188] Taken together, the convention and recommendations reflect a serious European-wide commitment to data protection in the medical domain.

In addition to the Council of Europe's convention and recommendations, the treatment of health care information within Europe will soon be affected by the Commission of the European Union's Directive on Data Protection. This directive relies on

---

183. Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, no. 108 (Jan. 28, 1981), Article 6 (*"European Convention"*).

184. Id. at Articles 5, 7, 8.

185. Id. at Article 8(d).

186. Council of Europe, *Regulations for Automated Medical Data Banks*, Recommendation No.R(81)1 (Jan. 23, 1981). The Explanatory Memorandum to the Recommendation states:

> the operation of every automated medical data bank [should be] subject to a specific set of regulations. The general purpose of these regulations should be to guarantee that medical data are used not only to ensure optimum medical care and services but also in such a way that the data subject's dignity and physical and mental integrity are fully respected.

Id. at 13.

187. Id. at 7.

188. See Project Group on Data Protection, Report, CJ-PD (93) 37 (Strasbourg, 17 Sept. 1993) (*"Draft Recommendation"*).

domestic legal institutions for its transformation into law.[189] Yet, in contrast to the Council of Europe's Convention on Data Protection, the Directive on Data Protection offers a more powerful vehicle for harmonization of European law through its greater detail and the possibility of direct reliance on the directive should it not be implemented correctly into domestic law.[190]

An amended draft of this document provides insights into the European Union's likely ultimate approach to medical data protection.[191] Like the convention, the Draft Directive requires member countries to establish legislation that conforms with its standards. Its goal is to ensure a "high level of protection" within the Union for "fundamental rights and freedoms, notably the right to privacy."[192] The directive stresses that fair information practices must be in place before member states permit the processing of personal information, including "data concerning health."[193] Put another way, without sufficient data protection, the processing of medical information may not occur.

The proposed directive and the Council of Europe's convention are of great significance. They are important in the first instance as positive examples of data protection measures for medical data. They are also important because they set rules not only for the processing of personal data *within* the European Union, but also for the transfer of these data to any "third country," including the United States.[194]

The council's convention and the Union's directive permit the prohibition of data transfers, including those involving medical information, to countries with insufficient data protection.[195] According to the Council of Europe's convention, a signatory nation may prohibit data transfers to third countries that occur "through the intermediary of the territory of another Party."[196] Such *indirect* transfers can be blocked when they would cause the circumvention of specific height-

189. George A. Bermann, Roger J. Goebel, William J. Davey, and Eleanor M. Fox, *Cases and Materials on European Community Law* 278 (West, 1993).

190. Stephen Weatherill and Paul Beaumont, *EC Law* 32, 116-17, 296-99 (Penguin, 1993).

191. Commission of the European Communities, *Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM(92)–SYN 287 ("*Draft Directive*").

192. Id. at Preamble (1).

193. Id. at Article 8.

194. Id. at Article 26.

195. Id.; *European Convention*, Article 12 (cited in note 183).

196. *European Convention*, Article 12 (3)(b).

ened regulations for certain categories of data.[197] Although the convention does not discuss the treatment of *direct* transfers to third countries,[198] the council's Draft Recommendation on the Protection of Medical Data does. It requires domestic legal provisions which are "in conformity with [the] Convention" before permitting a transfer of personal information to a state which has not ratified the treaty.[199]

The draft directive gives responsibility to each national government within the Community to oversee the conditions of transfers to non-Community nations. Its critical requirement is that data transfers be permitted "only if the third country in question ensures an adequate level of protection."[200] The adequacy of protection is to be "assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations."[201] Among the circumstances to be assessed are "the legislative provisions . . . in force in the third country in question."[202] The adequacy of protection can also depend on "professional rules," such as a given company's business practices or code of conduct.[203]

Data exports can also be limited under the laws of various European nations. The French Law on Data Processing, Data Files, and Individual Liberties allows the French data protection agency, the National Commission on Informatics and Liberties, to prohibit the transfer of information from France to foreign nations.[204] In one instance, the commission prevented Fiat from transferring employee data from France to Italy.[205] In Germany, the Federal Data Protection Law requires consideration of the data protection provided by a third country before any international transmission of personal informa-

197. Id. at Article 12(3)(a). For analysis of this provision of the convention, see Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transitional Financial Services*, 60 Fordham L. Rev. S137, S161-62 (1992).

198. The convention has, however, been interpreted as requiring equivalent protection in non-signatory nations. Spiros Simitis, *Datenschutz und Europäische Gemeinschaft*, 6 Recht der Datenverarbeitung 3, 11 (1990).

199. *Draft Recommendation* at 11.4 (cited in note 188). The *Draft Recommendation* adds that such transfers may occur even in the absence of such conformity if "a. necessary measures, including of a contractual nature, to respect the principles of the Convention and this Recommendation have been taken and the data subject has the possibility to object to the transfer, or b. the data subject has given his consent." Id.

200. *Draft Directive* at Article 26(1) (cited in note 191).

201. Id.

202. Id.

203. Id.

204. French Data Protection Law at Article 24, in *Data Protection Statutes* (cited in note 156).

205. Commission nationale de l'informatique et des libertés, 10e rapport d'activité 32-34 (1991).

tion.[206] Such analysis must be carried out in transfers by the government and private companies alike.[207] In cases of non-governmental transmissions, a private company may be subject to fines and even criminal penalties for transmissions from Germany to countries with insufficient protections.[208]

What do these provisions for blocking data exports under the Council of Europe's convention, the Union's directive, and national laws mean for the United States? They indicate that transfers of personal data from Europe to America depend upon the adequacy of protection that such data receive once transferred here. The decision whether to transfer is likely to be made after examining the nature of the data, the type of protection offered by the legal order, and the business practices in the United States.[209]

Medical data likely to be affected by these measures are found in a number of areas. To begin with, international corporations often send employee records containing health information from one country to another.[210] Moreover, there exists an international industry in information processing. American companies are part of this industry; they compete globally for contracts that involve the processing of health information.[211] American litigants also seek personal medical information from Europe through discovery motions. American courts must now weigh the effect of foreign data protection statutes in evaluating the permissibility of contested international discovery actions involving personal information.[212] Indeed, the Supreme Court

---

206. German Data Protection Law §§ 17, 28 (cited in note 157). For a discussion of the need for equivalent protection before the transfer of personal data from Germany to a foreign country, see Spiros Simitis, § 1 *(Räumlicher Geltungsbereich)*, in Spiros Simitis, Ulrich Dammann et. al. eds., *Kommentar zum Bundesdatenschutzgesetz*, § 1, Rdnr. 74-107 (4th ed. 1992).

207. German Data Protection Law §§ 43, 44. An individual section in the Social Law regulates international transmissions of personal data in the control of social welfare agencies, see Code of Social Law, Tenth Book § 77 (cited in note 158). This statute permits such transmission to be made only for a limited number of statutorily authorized purposes and only when there is no negative effect on an interest of the individual that is worthy of protection. Id.

208. Id.

209. *Draft Directive* at 26(2) (cited in note 191). For a description of the necessary analysis, see Spiros Simitis, *Datenschutz und Europäische Gemeinschaft*, 6 Recht der Datenverarbeitung 3, 20 (1990).

210. Such information was present in the Fiat case discussed above. See note 205 and accompanying text.

211. See generally Priscilla M. Regan, *The Globalization of Privacy: Implications of Recent Changes in Europe*, 52 Am. J. of Econ. & Soc. 257, 264-65 (1993).

212. See generally *Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, 546 (1987) (concerning the multi-factor balancing test to be applied to decide whether foreign parties must comply with a discovery request forbidden by foreign law).

has held that American courts have a special responsibility to "demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operation, and for any sovereign interest expressed by a foreign state."[213] The Supreme Court has approved a multi-factor balancing test to be applied in deciding whether foreign parties must comply with a discovery request that is forbidden by their domestic law.[214] Under this balancing test, foreign data protection laws should be entitled to great deference due to the importance foreign nations place on privacy protection.[215]

Finally, American drug companies market their products internationally. Because drugs tend to be approved more rapidly in Europe than in the United States, personal medical information from Europe can have an important role in the regulation of pharmaceutical products in this country.[216] In fact, the Food and Drug Administration even requires companies whose products have been approved to share information regarding "all adverse drug experience information obtained or otherwise received by the applicant from any source, *foreign* or domestic. . . ."[217] Yet, access to this information may be limited if foreign countries believe American protections inadequate.

Thus, the weaknesses in data protection law in the United States may lead to a blockage of international transfers of data to this

---

213. Id. at 544-46. See also Restatement (Third) of Foreign Relations Law of the United States § 437(1) (ALI, 1987).

214. *Societe Nationale*, 482 U.S. at 544 n. 28. See also *Richmark Corporation v. Timber Falling Consultants*, 959 F.2d 1468, 1476 (9th Cir. 1992).

215. *Societe Nationale*, 482 U.S. at 544 n. 28. Foreign data protection laws are to be regarded not as "blocking statutes," such as have been developed in the context of antitrust laws, see generally Note, *Foreign Nondisclosure Laws and Domestic Orders In Antitrust Litigation*, 88 Yale L. J. 612 (1979); Timothy G. Smith, Note, *Discovery of Documents Located Abroad in U.S. Antitrust Litigation*, 14 Va. J. Int'l Law 747 (1974), but as "substantive laws at variance with the law of the United States." *Societe Nationale*, 482 U.S. at 544 n. 29 (cited in note 213) (quoting Restatement (Third) of Foreign Relations § 437 (Reporter's Note 5 at 41) (cited in note 213)).

216. This point was made clear by a scandal in the early 1980s involving the drug benoxaprofen, which was marketed by Eli Lilly under the tradename Oraflex. Information from the United Kingdom indicated adverse drug reactions to this product, and a Congressional hearing before the Committee on Government Operations probed the issue of whether Lilly had promptly shared this information with the FDA. See The Regulation of New Drugs by the Food and Drug Administration: the New Drug Review Process, Hearings before a Subcommittee of the House Committee on Government Operations, 97th Cong., 2d Sess. 76-84 (1982).

During these hearings, the head of the Food and Drug Administration noted that privacy issues lead "many countries [to] hesitate to give us in the FDA certain information which they consider as privileged—and under their law is—and that they think might be helpful to us scientifically." Id. at 121.

217. 21 C.F.R. 314.80(b), (c) (1994) (emphasis added).

country.[218] Even when such transfers are not forbidden, the transactions in which they are involved will be subject to heightened scrutiny. The inevitable result of these blockages and this scrutiny will be dramatically increased costs to American businesses and litigants with interests in personal information from Europe. In the absence of federal protection of medical data, the flow of personal data from Europe to the United States will be less rapid, less regular, and associated with greater economic costs. It makes economic sense for the United States to institute federal data protection measures for medical data. Without such measures, American enterprises will be at a competitive disadvantage.

IV. TOWARD AN AMERICAN DATA PROTECTION LAW

Clearly, the United States has not been successful in protecting the privacy of health care information. However, a core of fair information practices can be ascertained by considering other areas of domestic law and by looking at European law. Four important elements of the necessary American data protection law can be identified: (1) the creation of a statutory fabric that defines obligations with respect to the uses of personal information; (2) the maintenance of transparent processing systems; (3) an assignment of limited procedural and substantive rights to the data subject; and (4) the establishment of effective governmental oversight of data use. These elements must be set out in legal standards that control the collection and use of personal medical information.

A. Creation of a Statutory Fabric of Defined Obligations

The first important element in the regulation of American health privacy is the creation of a statutory fabric that defines obligations with respect to the uses of personal information.[219] The goal of these obligations regarding data processing is to respect and encourage the individual's personal autonomy. But, any assignment of rights to individuals must be limited in scope. The law should not create an absolute right of control or a quasi-property interest in one's

218. Regan, 52 Am. J. of Econ. & Soc. at 264-65 (cited in note 211).

219. The Privacy Protection Study Commission has stated that privacy protection depends on legislation and other forms of regulation that "create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual." Privacy Protection Study Commission, *Personal Privacy* at 15 (cited in note 66).

personal data. Such an approach would do more harm than good because of the variety of critical social interests that can support access to any individual's personal data. Any rights in personal data must be anchored within a larger statutory setting of limits on how personal health care information can and cannot be used.

From this perspective, a critical problem with the current legal regulation of medical information is that it is centered around discrete health care relationships rather than health care data. As a result, data that are subject to statutory protection in the hands of one entity, such as a physician or hospital, may be largely free from legal controls once transferred to another actor, such as an insurance company.[220] A statutory scheme that effectively controls medical data must be tied to and follow the data throughout their different uses. Once identifiable health information is created or used during the process of medical treatment or payment, it should remain *protected* health information that is subject to fair information practices.

A statutory fabric to protect health care information must include the definition of a core set of responsibilities for those who process such information. Indeed, those who handle the information should be considered "trustees" whose responsibilities are statutorily defined.[221] Here, the law should center its attention on both the *use* and the *disclosure* of information. Use of health care information should only be permitted for reasons that are compatible with the purpose for which the information was collected. The principle of compatibility requires a significant degree of convergence—a concrete relationship—between the purpose for which the information was gathered and its subsequent use.[222]

Disclosure of health data should only be allowed for statutorily authorized purposes or with the patient's informed consent. Here, careful drafting will be necessary so that disclosure standards contain some measure of flexibility without creating loopholes that will permit

220. See David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* 125 (U. of Illinois, 1989) (arguing that laws regulating the insurance industry "need to be more comprehensive, covering personal privacy protections in all their dimensions").

221. The Code of Fair Information Practices for Health Information before the House of Representatives in the last Congress developed at some length this concept of a "trustee" for health care information, see H.R. 4077, 103d Cong., 2d Sess. (March 21, 1994) §§ 3, 101, 102, 111. See also 141 Cong. Rec. E63 (daily ed. Jan. 9, 1995) (reintroducing this legislation in the 104th Congress). Health care professionals are, in fact, already considered to be fiduciaries with a special duty to disclose all information to the patient which materially affect her rights and interests. See, for example, *Arato v. Avedon*, 5 Cal. 4th 1172, 858 P.2d 598, 602 (1993).

222. For important decisions developing this concept within the context of the Privacy Act, see *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 549-50 (3d Cir. 1989); *Covert v. Harrington*, 876 F.2d 751, 753 (9th Cir. 1989).

abuse of privacy. The most critical categories of statutorily authorized disclosures are: (1) for treatment and payment; (2) for quality control (including physician monitoring); (3) to next of kin (if such disclosure is consistent with accepted medical practice);[223] (4) for public health reporting; (5) for health research; and (6) for law enforcement purposes. Each statutory category should articulate the limited conditions under which the permitted disclosure is to take place.

The kinds of conditions to be placed on these authorized disclosures may be illustrated with reference to health research projects and public health reporting. In the United States, academic health research projects are already reviewed by institutional boards for compliance with a variety of ethical standards.[224] Drawing on this established safeguard, a health research disclosure must be made only to projects that have already met with the approval of an independent institutional review board or similar entity. The health reform bill of Senator George Mitchell proposed the establishment of a process by which the Secretary of Health and Human Services would certify institutional review boards in the public and private sectors.[225] The certification process would insure that the review boards would have the "qualifications to . . . protect the confidentiality of research subjects."[226] Part of the activity of review boards is to insure that at the earliest possible date all identifiable information used in health research projects be turned into aggregate data that cannot identify particular individuals.

---

223. To be sure, this practice is not entirely settled. Considerable debate has taken place concerning disclosures of HIV information to partners. See Roger Doughty, *The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic*, 82 Cal. L. Rev. 113, 163-75 (1994). See generally Edgar and Hazel Sandomire, *Medical Privacy Issues in the Age of AIDS: Legislative Opinions*, 16 Am. J. L. & Med. 155 (1990); Richard C. Turkington, *Confidentiality Policy for HIV-Related Information: An Analytical Framework for Sorting Out Hard and Eacy Cases*, 34 Vill. L. Rev. 871 (1989).

In the context of abortion, the Supreme Court bas held unconstitutional a state requirement that a pregnant woman sign a statement indicating that she notified her husband of her intention to obtain an abortion, *Planned Parenthood of Southeastern Pennslyvania v. Cascy*, 112 S. Ct. 2791, 2830 (1992), and upheld a requirement that one parent give informed consent before a pregant minor can obtain an abortion—so long as this law also contains a judicial bypass procedure. Id. at 2832.

224. Kathryn Kelly and Sara Jones, *Tort Liability, Immunities, and Defenses*, in Anne M. Dellinger, ed., *Healtheare Facilities Law* 257, 368-77 (Little, Brown, 1991).

225. Health Security Act, Mitchell Amendment No. 2560 to S.2351, § 5218(c)(2), in 140 Cong. Rec. S11492, S11595 (daily ed. Aug. 12, 1994).

226. Id.

Disclosure for the purpose of public health reporting should only be permitted pursuant to an acceptable public health reporting statute. Such a statute must contain specific sufficient limitations on the use of health care information. These safeguards must include limitations on the time for which these data may be stored in individually identifiable form. Such standards would provide a powerful incentive for state legislatures to redraft the public health reporting laws that are currently couched in broad or vague terms. The drafting of such carefully crafted conditions for disclosure is absolutely essential; in addition, other protections will be needed to prevent abuse of the notion of informed consent. Part IV.C discusses the content of these safeguards.

B. The Maintenance of Transparent Processing Systems

The second element of an American data protection law, the maintenance of transparent processing systems, requires that the use of personal information be structured to make it open and understandable to citizens.[227] An open data protection law requires the state to organize the processing of personal information in a manner that encourages self-determination. While secret files and the impenetrable ways of computers discourage decision making and provide opportunities to coerce the individual, an understanding of how information is obtained and used encourages citizens to assert themselves in the spheres of social and political life.

The transparency element of a data protection law requires that citizens understand how their medical information will be used. This knowledge should be imparted through a "notice of information practices" that is given to individuals. American law already has some experience with such documents; the Privacy Act requires use of such a notice mechanism.[228] A health care data protection act should

227. In the words of the Privacy Protection Study Commission in 1977, an effective privacy policy must "open up record-keeping operations." Privacy Protection Study Commission, *Personal Privacy* at 14 (cited in note 66). This body's official report stated, "The Commission believes that by opening up record-keeping practices and by giving an individual opportunities to interact easily with a record keeper, particularly at crucial points in a record-keeping relationship, both individuals and organizations will benefit." Id. at 19.

228. See 5 U.S.C. § 552a(e)(3) (1988). The Privacy Act requires an agency to "inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separato form that can be retained by the individual" of the legal authority authorizing the solicitation of the personal information, the principal purposes for which the information will be used, the routine uses planned for the information, and the effects, if any, of not providing the personal information. Id. Unfortunately, the Privacy Act has not created effective notice of federal data use. See Flaherty, *Protecting Privacy* at 341 (cited in note 8) (explaining that the general public is unaware of the protections the Privacy Act affords). Part

establish a notice requirement with four elements, the first two describing the individual's rights and the last two specifying the purposes of collection.

First, the notice requirement must provide a description of the individual's rights, including the extent of access provided to her own records. Second, notice must include an explanation of the procedures under which these rights can be exercised. Part of a patient's general right to inspect and possess a copy of her medical information should include the power to seek correction of any health information that is not timely, accurate, or complete.[229] Third, the notice requirement must give an explanation of the purposes for collection of personal medical data.[230] The patient should know how and by whom this information will be used.[231] Fourth, and finally, the notice requirement must include a specification of the extent of the authorized disclosure of collected data. This specification would explain the nature of the authorization of disclosures and the substantive limits on additional unrelated use of the information. Only this knowledge, provided by the notice requirement, would allow the individual to play a role in preventing collection, storage, and use of unnecessary information.[232]

C. Assignment of Limited Procedural and Substantive Rights

The third element of an American data protection law is the assignment of limited procedural and substantive rights to the individual. As has been previously noted, an individual's control over medical or other personal information cannot be absolute. Therefore, the role of data protection law is to shape personal rights to reflect a balance between individual and social interests in medical data.

---

of the problem is that the limited nature of remedies offered under the Privacy Act reduces the importance of the procedural and substantive interests assigned by this statute to the individual.

229. Narrowly crafted statutory exceptions to this right of inspection should exist for some data, the most important of which are certain kinds of mental health treatment records.

230. Such a requirement is known to both European and United States law, see the *European Convention* at Article 14(3)(c) (cited in note 183); Privacy Act, 5 U.S.C. § 552a(e)(3) (1988).

231. For shortcomings in the execution of such explanations in the context of American welfare law and child support enforcement, see Schwartz, 43 Hastings L. J. at 1352-74 (cited in note 8).

232. See Bennett, *Regulating Privacy* at 156-58 (cited in note 8) (discussing necessary support for "subject control" model of data protection).

1. Procedural Rights

Procedural interests of the individual in personal medical information include: (1) the right to be informed whether one is required to supply medical information; and (2) the right to have a mechanism by which one can inspect and correct data. Such procedural rights also serve to guarantee the transparency of data processing.[233]

The assignment of rights to the individual also requires the shaping of effective remedies. A modern remedial scheme should entail three kinds of protections. First, any individual whose interests under a health care information practices law have been violated must be permitted to bring a civil action with the possibility of monetary penalties. Second, methods of alternative dispute resolution should be available to encourage affordable relief and timely resolution of claims.[234] Third, violations of certain fair information practices should be punishable by criminal penalties. For example, criminal sanctions should apply to the obtaining of protected health care information under false pretenses with the intent to apply such information for monetary gain.

2. Substantive Rights

Informed consent to the use of medical data is another important individual right. In the context of physical treatment, the meaning of informed consent is far from settled. In a recent analysis of the doctrine, Peter Schuck has differentiated between two forms of informed consent: one version developed by "idealists" and the other version developed by "realists."[235] Informed consent idealists advocate an expansive obligation of the physician to disclose information about risks and alternatives and also concentrate on the patient's actual

---

233. Transparency is the second necessary element of an adequate data protection law. See Part IV.B.

234. For a discussion of the application of alternative dispute resolution within the context of medical malpractice, see Kelly and Jones, *Tort Liability* at 377-86 (cited in note 224). The Workgroup for Electronic Data Interchange has also stressed the potential contribution of alternative dispute resolution mechanisms in resolving disputes about fair information practices. Workgroup for Electronic Data Interchange, *1993 Report* at 3–9 (cited in note 44).

235. Peter H. Schuck, *Rethinking Informed Consent*, 103 Yale L. J. 899, 902-04, (1994). For an example of the idealists, see generally Jay Katz, *The Silent World of Doctor and Patient* (Free, 1984); for an example of a realist, see Joseph Goldstein, *For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent and the Plea Bargain*, 84 Yale L. J. 683, 690-94 (1975).

knowledge or understanding in giving consent.[236] In contrast, informed consent realists emphasize "the process of informing the citizen for decision."[237] Realists focus on developing objective standards concerning the conduct of the informing authority.

Whatever the merits of the different sides of the debate regarding "informed consent" before physical treatment, the realist view is preferable for disclosure concerning data processing. As Schuck notes, "most health care in the future will be delivered in a highly bureaucratic-technocratic context."[238] Under these circumstances, it makes little sense to require that informed consent to data processing be based on a physician and patient engaging in a dialogue that will lead to shared decision making about the application of the patient's personal information. In fact, the health care provider and patient are already required to disclose, without the patient's express consent, medical data for many data processing uses. For example, the physician and patient cannot agree to opt out of sharing information with the third party payor; society has also made the judgment that data must be shared under certain circumstances for epidemiological or other public health purposes.

Informed consent to the release of personal data requires "the process of informing for agreement."[239] This language means that health care providers must provide patients with information regarding specific planned uses of personal medical data. In light of the current abuse of informed consent through the use of blanket disclosure documents, careful new safeguards are required. These safeguards should anchor the right of informed consent within a legal framework of standards for use and disclosure of data and also include limits on the conditions under which the process of informing for agreement is to take place.

In establishing this new approach, the law should also reconsider its current overreliance on the concept of written documentation of informed consent. Blanket consent forms, while written, are inadequate to obtain truly informed consent. Health care data should only be processed for a statutorily authorized purpose or with the patient's informed consent. This approach requires the articulation of a limited set of statutory conditions under which permitted use or disclosures may occur. Once patients are informed about the planned

236. Schuck, 103 Yale L. J. at 903; Katz, *The Silent World* at 165-206.
237. Goldstein, 84 Yale L. J. at 692 (cited in note 235).
238. Schuck, 103 Yale L. J. at 926 (cited in note 235).
239. See Goldstein, 84 Yale L. J. at 692 (cited in note 235).

use of their information, it may be used only in these statutorily defined circumstances. Once a health care provider gives information regarding the planned use, including an explanation of the "notice of fair information practices," the patient's consent to an application for a statutorily defined purpose need not be memorialized in writing. In circumstances in which a use or disclosure is not statutorily authorized, formal documentation of consent will be required. This approach will lead individuals to scrutinize closely all situations in which they are asked to sign consent documents for the use of their health care information.

Additional safeguards may sometimes be needed to insure that consent is given in a process that is informative. In circumstances in which formal documentation of informed consent is required because a nonauthorized use or disclosure is involved, consent may not be given on the same day that the individual seeks health care. Moreover, the provision of care may never be made contingent on the signature of the consent document for a nonauthorized purpose. In addition, any consent should only remain valid for a limited period and for a purpose that has been explained to the patient in writing.[240] This approach to informed consent has considerable merit in requiring written authorizations only in situations in which patient scrutiny is most critical. In all situations where protected health information is generated, however, patients are to receive notice of the planned data uses and have an opportunity to refuse consent.

D. Establishment of Governmental Oversight

The fourth and final element of an American data protection law is government monitoring of information processing. The protection of informational self-determination in an age of rapid technological change mandates the creation of a governmental body with the institutional expertise and continuity of interest to understand the impact of changes in this area and draw attention to the need for improvements in legal regulation.[241] This oversight is particularly important in the medical sector where the greatest changes in personal data use are likely to take place. The idea of creating such an

240. These safeguards are already contained in the provisions that protect confidentiality in the records of federally funded suhstance abuse clinics, see notes 127-29 and accompanying text.

241. For further discussion of the need for a data protection board, see Schwartz, 43 Hastings L. J. at 1379-86 (cited in note 8); Office of Technology Assessment, *Protecting Privacy in Information* at 86-87 (cited in note 33).

institution has been part of policy discussions since the debate preceding the creation of the Privacy Act in 1974[242] and is likely today to receive particularly strong support from the American people. A 1993 poll indicated that eighty-six percent of the American public favored the creation of an "independent National Medical Privacy Board" that would "hold hearings, issue regulations, and enforce standards."[243]

Drawing on past American legislative proposals and the international experience with such institutions, it is possible to spell out the duties of a United States Data Protection Board. Ideally, such an entity would be a general privacy protection agency rather than one restricted to health care issues. This broader authority is needed because informational privacy issues are cross-sectoral in nature.[244] The regulation of health care data, for example, raises issues not only in health law but also in administrative law, labor law, and fair credit law. Therefore, the creation of a general United States Data Protection Board would heighten the administrative expertise necessary to provide proper oversight of health care data.

A United States Data Protection Board would be of assistance to numerous social groups. Its monitoring of both data processing practices and compliance with laws would draw the attention of the legislature and the public to weaknesses in existing laws and assist citizens seeking to protect their interests and exercise their rights. The board would also help businesses understand and comply with legal requirements. By fulfilling these tasks, the data protection commission would keep public administrators, the legislature, citizens, and the business community aware and involved in the debate over privacy as new conflicts generated by information technology emerge.

A further role of a Data Protection Commission would be to represent American interests and assist American companies who face scrutiny by foreigu data privacy authorities. Virtually all other Western nations have created such agencies for data protection over-

242. See H.R. Rep. No. 93-1416, 93d Cong., 2d Sess. (1974), reprinted in U.S. Congress, *Legislative History of the Privacy Act of 1974*, 3-8 (1976) (*"Legislative History of Privacy Act"*) (remarks of Senator Sam Ervin introducing a bill to establish a Federal Privacy Board). The policy debate at this time has been explored by Flaherty, *Protecting Privacy* at 310-15 (cited in note 8) and Bennett, *Regulating Privacy* at 170-73 (cited in note 8).

243. *Health Information Privacy Survey* at 11 (cited in note 1).

244. Data protection boards in Europe and Canada are, in fact, constructed on this generalist model, see Flaherty, *Protecting Privacy* at 21-26, 93-101, 165-72, 243-48 (cited in note 8); Paul M. Schwartz, *Administrative Law: The Oversight of Data Protection Law*, 39 Am. J. Comp. L. 618, 619 (1991) (book review of Flaherty, *Protecting Privacy*).

sight.[245] Indeed, the European Commission's Draft Directive requires each member state to "designate an independent public authority to supervise the protection of personal data."[246] Significant formal and informal contacts now occur regularly between the world's data protection commissioners.[247] The United States needs to create an American Data Protection Commission before it can play a full role in these important international discussions.

In the current political environment, considerable opposition exists to the creation of an additional federal institution for any reason. Americans are suspicious of their government and do not wish to create any more bureaucracy.[248] Meetings of the world's data protection commissioners indicate, however, that this hostility toward state activity limits American participation in the important world discussion about international data transfers. In a broader sense, deliberative autonomy is not merely a pre-existing quality whose protection requires an *absence* of state power. Protection of medical privacy requires that difficult choices be made regarding the structuring of the flow of personal data. A data protection board can play a critical role in ensuring that these decisions be made in a fashion that will further informational autonomy.

E. Responding to Current Abuses of Medical Privacy

Creation of an American data protection law satisfying these four elements would respond to the abuses that this Article has identified. The appropriate response must remedy two types of abuses: (1) the trafficking of lists of health care information by direct market mailers; and (2) employer access to worker medical data through wellness programs and health insurance plans. After considering the response to these two situations, this Part discusses two bills introduced in the last Congress whose passage is essential to the creation of an adequate law for protection of health care data.

First, the marketing of lists of health care data must be blocked by a federal health care data protection act.[249] This law

245. Flaherty, *Protecting Privacy* at 21-29, 93-103, 165-74, 243-52.

246. *Draft Directive* at Article 30 (cited in note 191).

247. An important number of these contacts occur at the Annual Meeting of Data Protection Commissioners. The 1994 meeting in the Netherlands marked the sixteenth year that this official encounter has taken place among the world's data protection commissioners.

248. See Schuck, 103 Yale L. J. at 901 (cited in note 235) (noting Americans have an "abiding, almost obsessive suspicion of state power").

249. Some attempts at self-regulation by the direct marketing industry have taken place. The Direct Marketing Association ("DMA") has created an opt-out provision for individuals,

should *not* contain a statutory authorization for the disclosure of health care information to direct market mailers. Rather, statutory authorizations should be limited to a core minimum of necessary or highly useful social applications. Although receiving product mailings and telephone solicitations might reduce the information costs of consumers, American law, to the extent that it has considered the issue, has not generally found this interest to be important enough to permit unrestricted release of personal information. A recent Supreme Court decision is illustrative of this point.

In *Department of Defense v. Federal Labor Relations Authority*,[250] the United States Supreme Court reviewed an attempt under the Freedom of Information Act by two unions to obtain the home addresses of federal agency employees from the Department of Defense. These employees had been designated as belonging to bargaining units represented by the labor organizations. The Supreme Court identified a significant privacy interest in the nondisclosure of the names and addresses of the workers.[251] The Court found that this privacy interest was protected under the Freedom of Information Act's Section (b)(6) disclosure exemption. In fact, the access that "commercial advertisers and solicitors" would have to this information was an important factor for the Supreme Court in evaluating the weight of the privacy interest at stake.[252] In its opinion, the Court also emphasized the importance of "the interest that individuals have in preventing at least some unsolicited, unwanted mail from reaching them at their homes."[253] It found that the Department of Defense was prohibited from releasing the information to the two unions.

Just as no statutory authorization should permit the *disclosure* of health care information to direct market mailers, the normal *use* of these data by physicians and hospitals should not entail such a release. Such a use is not compatible with the purpose for which physi-

---

industry guidelines, and a privacy manual for direct marketers. See Direct Marketing Association, *Fair Information Practices Manual* (1994); Paul M. Alberta, *DMA Unveils Privacy-Practices Book*, Direct Marketing News 6 (Aug. 8, 1994).

Considerable doubt exists as to the extent of consumer knowledge of the opt-out provision and the extent to which the industry is committed to compliance with the DMA's guidelines. See Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. ___ (1995) (forthcoming). Indeed, Metromail, a member of the Privacy Task Force of the DMA, created profiles of millions of Americans with specific health conditions. See id.; Ray Schulz, *Carlson, Metromail Offer Medical Data*, Direct Marketing News 2 (June 21, 1993).

250. 113 S. Ct. 1006 (1993).

251. Id. at 1016.

252. Id. at 1015.

253. Id.

cians and hospitals gather information. Thus, direct market mailers should only be able to obtain protected health care information with the written consent of patients. Here, too, all the safeguards for the documentation of informed consent should apply. This approach would prevent health care information from being obtained by such means as caller identification devices attached to the toll-free numbers of pharmaceutical companies that supply product information.[254] If individuals wished their medical information to appear on direct market lists, they would have to give their formal written consent and thereby "opt-in" to this use of their data.

Second, under the protection of a federal health care privacy statute, significant changes should occur in how worker data are used within employee wellness programs and health care plans. Health care data generated for counseling or treatment purposes should not generally be released to nonmedical company personnel or used for purposes that are not compatible with the reason for which the information is collected. Although this approach to health care privacy will result in changes at a number of corporations, at least one company, International Business Machines ("IBM"), already has adopted an approach consistent with these practices.[255] Moreover, IBM has found that privacy protection is a fiscally sound policy. In recent testimony at congressional hearings on medical privacy, a representative of IBM stated, "The fact that we have been able to continue to provide our employees a broad array of medical benefits at reasonable costs while operating with these self-imposed restrictions is proof that maintaining high standards of confidentiality need not compromise efficiency."[256] Respect for privacy in the administration of health care benefits need not be at the cost of fiscal health.

The response to the current abuses in health care privacy that this Article advocates is within the reach of American law. Two bills that were before the 103d Congress properly expressed the four essential elements of an American data protection law that this Article has developed. The first bill, the Fair Health Information Practices Act of 1994,[257] expressed the first three of the four principles necessary to an effective American data protection law. It provided for transparency

---

254. Compare Ballinger, Direct Marketing News at 1 (cited in note 73).

255. See Linowes, *Privacy in America* at 30-31, 122 (cited in note 220).

256. Fair Health Information Practices Act of 1994, Hearing on H.R. 4077, before the Subcommittee on Information, Justice, Transportation and Agriculture of the House Committee on Government Operations, 103d Cong., 2d Sess. 7 (May 4, 1994) (Statement of Dr. Richard Barker and Dr. Martin Sepulveda).

257. H.R. 4077, 103d Cong., 2d Sess. (cited in note 221). The bill was reintroduced in the 104th Congress. See note 221.

of data processing systems by allowing patients to receive both a copy of medical information about themselves and a notice of information practices that describes their rights and the authorized uses and disclosures of health information. The Fair Health Information Practices Act also created a statutory fabric of defined obligations with respect to possible uses and disclosures of personal information. It established uniform rules that apply to all health care information that is used or created during the medical treatment or payment process.[258] Such information becomes protected health data subject to statutory regulation. Finally, this bill assigned important procedural and substantive rights to the individual.[259] Among these rights is the ability to seek correction of one's health information if it is not timely, accurate, or complete.[260] The Fair Health Information Practices Act represents an excellent start in creating an American data protection law for medical information.

Second, a bill which would create an effective, general data protection board, was introduced in the last Senate.[261] Similar bills have been previously before the House of Representatives,[262] but Congress also failed to promulgate this measure. Yet, health care

---

258. H.R. 4077, 103d Cong., 2d Sess. at §§ 101-130.

259. Id. at §§ 111-115; 161-164.

260. Id. at §§ 111-112.

261. Privacy Protection Act of 1993, S. 1735, 103d Cong., 1st Sess. (Dec. 1, 1993), in 139 Cong. Rec. S16494 (daily ed. Nov. 19, 1993). This Bill offers a superior structure for data protection oversight than the Bill considered in the House (Individual Privacy Protection Act of 1993, H.R. 135, 103d Cong., 1st Sess. (Jan. 8, 1993)).

In contrast, the Clinton Health Security Act set up two administrative entities with responsibilities for oversight of the processing of health care information. Here, the problem is that these bodies are structured in ways that make them unlikely to prove fit for the required tasks.

The first body with data protection responsibilities under the Clinton Health Security Act is the National Health Board. Health Security Act § 5101(a) (cited in note 11). Yet, an agency that seeks to limit health care spending and improve health care quality is not likely to be a zealous advocate of the creation of limits on the sharing of medical data. This entity is not likely to have spare institutional energy or political capital to devote to the protection of privacy. Indeed, these central institutional concerns are ones that may appear to conflict with data protection.

The Health Security Act also envisions the creation of a second body, a fifteen-member National Privacy and Health Data Advisory Council, with data protection responsibilities. Id. at § 5140(a), (b). Unfortunately, this group is to meet only three times a year, id. at §5140(a), and is likely, at best, to be a weak force in the decisionmaking process regarding the application of personal health care information. The United States needs an independent data protection board that is empowered to consider the effects and implications of data processing in the medical and other sectors.

262. See, for example, Data Protection Act of 1989, H.R. 3669, 101st Cong., 1st Sess. (Nov. 18, 1989); Individual Privacy Protection Act of 1989, H.R. 126, 101st Cong., 1st Sess. (Jan. 7, 1989); Introductory Remarks of Senator Ervin on S.3418, reprinted in *Legislative History of Privacy Act*, 3-8 (cited in note 242). A similar bill has been introduced in the 104th Congress. See Individual Privacy Protection Act of 1995, H.R. 184, 104th Cong., 1st Sess. (Jan. 4, 1995).

reform should be accompanied by both passage of a fair information practices act and by creation of such an agency. In its attempt to protect an individual's interest in personal health care information, data protection law will remain effective only if such an agency exists to assist government, the legislature, the business community, and citizens.

V. CONCLUSION

The processing of personal information already plays a critical role in the provision, regulation, and financing of medical services by government and private entities. Beyond the traditional doctor-patient relationship and the provision of health services in hospitals, a variety of public and private organizations now use personal medical data. Health care reform will, however, further increase the extent to which health care data are used and shared. As part of this process, greater use will be made of information technology in an attempt to control costs and increase the quality of care.

The heightened use of personal data in the provision of medical services increases the threat to the patient's right of informational self-determination. The risk is acute given American law's lack of success in regulating the use of health care information. The legal response to this situation should be a data protection law in which informed consent to information processing plays a role. Yet, any right of informed consent will only be effective when anchored within an overall legal set of rules for the processing of health care information.

This Article has argued that such rules should be established in an American data protection law. It has developed the four essential elements of this law: First, the law must create a statutory fabric that defines obligations for those who process health care information. Second, the law must require transparency, meaning that the individual must receive notice of the structure of the processing of her personal data. Third, the law must assign limited procedural and substantive rights to the data subject. Citizens must know whether they are required to supply medical information and must know the mechanisms by which they can inspect and correct data. These procedural and substantive rights must also include the right to informed consent to uses of medical data and the right to receive suitable remedies for abuses of medical privacy. Fourth and finally, the American data protection law must ensure governmental oversight of

information processing. In an era of rapid technological change, a data protection board is necessary to carry out ongoing monitoring of technological developments and to advise the legislature of the extent of compliance with fair information practices. Such an agency is also needed to help citizens exercise their rights and to assist the business community in its response to national and international regulations.

According to Knock, the protagonist in a French farce, "People in good health are sick ones who don't know it."[263] All of us will need medical care at one time or another; indeed, a critical test of the fundamental fairness of a society is the manner in which it provides its citizens with such services.[264] Medical treatment inevitably leads, however, to the creation of a tremendous amount of health care information. When this information circulates without adequate protection, a strong negative pressure on the individual may arise and threaten the individual's ability to engage in critical reflection and join in communal life. Even mere uncertainty about social use of personal medical information can make individuals reluctant to seek preventative care. An essential part of any American health care reform must be a data protection law that improves how health care information is used, shared, and stored. Data protection law must be part of the prescription for the future health of the democratic order in the United States.

263. Jules Romains, *Knock ou Le triomphe de la Médecine*, Act I at 35 (Gallimard, 2d ed. 1985) (orig. ed. 1924) ("Les gens bien portants sont des malades qui s'ignorent").

264. Dworkin, 41 N. Y. Rev. of Books at 23 (cited in note 11) (discussing issues of justice in health care).