SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Health Matrix: The Journal of Law-Medicine

Volume 5 | Issue 1

1995

Privacy and Security of Health Information in the Emerging Health Care System

Lawrence O. Gostin

Joan Turek-Brezina

Madison Powers

Rene Kozloff

HEALTH MATRIX:
Journal of Law-Medicine

PRIVACY AND SECURITY OF HEALTH INFORMATION IN THE EMERGING HEALTH CARE SYSTEM

Lawrence O. Gostin†
Joan Turek-Brezina††
Madison Powers†††
Rene Kozloff††††

---

† Associate Professor of Law, Georgetown University Law Center and Professor, the Johns Hopkins University School of Hygiene and Public Health; Co-Director of Georgetown-Johns Hopkins Program on Law and Public Health. This paper is based on the work done by the authors for the health information and privacy committee of the President's Task Force on National Health Care Reform. The members of that committee were Lawrence O. Gostin (Chair), Joan Turek-Brezina, Madison Powers, Rene Kozloff, Ruth Faden, and Dennis Steinauer. The authors also would like to acknowledge the contribution of John P. Fanning of the U.S. Department of Health and Human Services and Barbara L. Looney, J.D./M.P.H. candidate, 1995, Georgetown University Law Center/Johns Hopkins University School of Hygiene and Public Health.. This article is based, in part, on Lawrence O. Gostin et al., *Privacy and Security of Personal Information in a New Health Care System*, 270 JAMA 2487 (1993), and Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. (forthcoming 1995).

Professor Gostin acknowledges the support of the U.S. Centers for Disease Control and Prevention, the Council of State and Territorial Epidemiologists, the Task Force on Child Survival, and a Dean's Scholarship award from the Georgetown University Law Center.

The positions stated in this article do not represent the policy of the President's Task Force on Health Care Reform or the U.S. Department of Health and Human Services Task Force on Privacy.

†† Ph.D.; Director, Division of Technical and Computer Support, Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services.

††† J.D., Ph.D.; Senior Research Scholar, Kennedy Institute of Ethics, Georgetown University.

†††† Ph.D.; Vice-President, KAI.

A COMPLEX HEALTH CARE information infrastructure is emerging in the American health care system. The success of the system will depend, in part, on the accuracy, correctness, and trustworthiness of the information and the privacy rights of individuals to control the disclosure of personal information. All participants in the new system (consumers and patients, health plans, and federal and state regulatory authorities) will need access to high quality information for informed decision making. At the same time, everyone must have confidence that information of a private nature is adequately protected.

American society places a high value on individual rights, autonomous decision making, and the protection of the private sphere from governmental or other intrusion. Concerns about privacy transcend the health care setting. Americans believe that their privacy rights as consumers are not adequately protected. In a 1993 Harris poll on consumer privacy conducted for Equifax, Inc., 78% of the respondents indicated their concern about threats to privacy. Eight out of ten respondents believed that consumers have lost all control over how personal information about them is circulated and used.[1] Public fear and distrust of both technology and bureaucracy is likely to increase as collection, storage, and dissemination of information becomes automated.

Health care information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual. As the U.S. health care system grows in size, scope, and integration, the vulnerability of that information also will increase unless protective measures are instituted.

This Article explains the objectives for the collection, storage, and use of information in the health care system and the means to attain those objectives.[2] The goals are to ensure (1) the *integrity* of health data so information is accurate, correct, and trustworthy — the integrity of information is critical to

1. LOUIS HARRIS AND ASSOCS., HEALTH INFORMATION PRIVACY SURVEY 22 (1993). *See also* LOUIS HARRIS AND ASSOCS., HARRIS-EQUIFAX CONSUMER PRIVACY SURVEY 1992, at 52 (1992).

2. *See generally* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L REV. (forthcoming 1995).

quality patient care, assessment of services, research, and public health; (2) the *availability* of health data so authorized persons who need the information for legitimate health purposes have ready access to the data — if clinical information is not readily available to health care providers, the best interests of patients may be significantly compromised; and (3) the *confidentiality* of health data so patients and consumers can be assured that personal information is only disclosed to authorized persons for authorized purposes at authorized times — identifiable data can be released only with the informed consent of the patient or consumer.

The goals of integrity, availability, and confidentiality of health care data can only be achieved by establishing an appropriate privacy and security framework. Although the definition of privacy and the nature of privacy rights are matters of philosophical controversy, privacy rights are understood as the right of an individual to limit access by others to some aspect of the person. This Article focuses on informational privacy so that information about a person is beyond the range of others without specific authorization.

Confidentiality is a form of informational privacy characterized by a special relationship, such as the physician-patient relationship. Personal information obtained in the course of that relationship should not be revealed to others unless the patient is first made aware and consents to its disclosure.[3] Security encompasses a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction and to safeguard the system itself.[4]

This Article first examines the needs for information in a modern health care system, including automated information. Second, a brief contemporary history of privacy law and policy is presented to show that the ideas are not new, but have been thoughtfully developed over time. Third, the ethical foundations for safeguarding privacy are explored so that changes in law and policy are consistent with sound ethical values. Fourth, a comprehensive set of fair information practices are presented

3. The terms privacy and confidentiality are discussed further at notes 64-71 *infra* and accompanying text.

4. The term security is discussed further at notes 80-85 *infra* and accompanying text.

that will guide all participants in the new system in the collection and use of confidential information. Fifth, the security of health information systems, particularly automated systems, is examined. Finally, the Article sets out a series of actions necessary for ensuring the integrity, availability, and confidentiality of health records.

I. HEALTH INFORMATION IN A MODERN HEALTH CARE SYSTEM

The collection and transmission of vast amounts of health information in automated form will occur with or without reform of the health care system. While comprehensive reform at the national level is unlikely for the immediate future, reform is taking place at the state level and within the private sector. A health care system in transition will create a need for additional information for monitoring patient care and assessing system performance. A modern health care system requires the sharing of a large volume of detailed health information among system players. The health information infrastructure that is being developed will have the following features that are critically important in providing high-quality, cost-effective health care, but required rigorous privacy safeguards.

A. Automated Health Information

The health care system will store and transmit more and more information in electronic form. Automation will support efforts to provide higher quality, cost-effective health care. Data collected will provide information needed for quality assurance, analysis of practice patterns and patient outcomes, and scientific research, all of which contribute to higher quality care. These data also can better inform consumers of their health care choices. Health care costs can be reduced by eliminating the need for duplicate tests, making it easier to detect fraud based upon more detailed examination of practice, and eliminating enormous paperwork burdens from patients, health care professionals, and health plans. Automation also supports the goal of portability of health coverage. Information will be readily available in a mobile society, as consumers move from provider to provider, plan to plan.

The ease of collection, storage, and transmission of data over electronic networks also creates significant risks to pri-

vacy. Health records contain a vast amount of personal information: demographic information such as age, sex, race, and occupation; financial information such as employment status, income, disabilities, and participation in federal or state programs; medical information such as diagnosis, treatments, and disease histories including mental illness, drug or alcohol dependency, AIDS, or sexually transmitted diseases (STDs); and social information such as family, sexual relationships, and lifestyle choices. This information is frequently sufficient to provide a detailed profile of the individual. Traditional medical records, moreover, are only a subset of automated records containing substantial health or personal information held by educators, employers, law enforcement, and government agencies.

The importance of privacy and security of automated records is widely acknowledged with numerous governmental and nongovernmental committees working on the issue, including the Congressional Office of Technology Assessment,[5] the Institute of Medicine,[6] the Physician Payment Review Commission,[7] and the U.S. Department of Health and Human Services (HHS).[8] A General Accounting Office (GAO) report recommends that the federal government set out national standards for the protection of automated health records.[9]

B. Health Cards and Unique Identifiers

Under many proposals for health care reform at the federal or state level, health cards would be issued to eligible persons entitling them to register in a health plan and to receive

---

5. *See* OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, OTA-TCT-576, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION (1993).

6. *See* MOLLA S. DONALDSON & KATHLEEN N. LOHR, INSTITUTE OF MEDICINE, HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY (1994).

7. *See* PHYSICIAN PAYMENT REVIEW COMM'N, ANNUAL REPORT TO CONGRESS 315-16 (1994) (citing OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5).

8. *See* WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, U.S. DEP'T OF HEALTH AND HUMAN SERVS., REPORT OF THE WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS TO THE SECRETARY OF THE U.S. DEPT. OF HEALTH AND HUMAN SERVICES (1993) (analyzing the risks and benefits to personal privacy inherent in computerization of health care information).

9. INFORMATION MANAGEMENT & TECHNOLOGY DIVISION, GEN. ACCOUNTING OFFICE, PUB. NO. GAO/IMTEC-93-17, AUTOMATED MEDICAL RECORDS: LEADERSHIP NEEDED TO EXPEDITE STANDARDS DEVELOPMENT: REPORT TO THE CHAIRMAN COMMITTEE ON GOVERNMENTAL AFFAIRS, U.S. SENATE 16-17 (1993) (recommending that Congress provide leadership to the private sector or elevate the role of federal agencies in developing standards).

services. Basic both to health care reform and to current efforts at developing electronic health care networks is the use of a unique identifier for each person. A unique identifier is necessary to help ensure the accuracy of information and efficient operation of the health care system. Perhaps the most critical single decision regarding privacy and security is whether to use the social security number (SSN) as the individual identifier. Most of the recent health care initiatives have proposed using the SSN as the unique personal identifier because it provides the most cost-effective way of identifying the individual and reliably collecting and sharing personal information.[10]

Many people in the privacy community object to the use of the SSN because of its extensive use for a large variety of non-health related purposes and its potential ability to link databases. Among the users of the SSN are debt collectors, department stores, utilities, check validation services, supermarkets, cable television, credit card issuers, banks, major oil companies, the Internal Revenue Service, other federal agencies (the military, the Parent Locator Service, food stamps, the Selective Service System), mailing list companies, credit bureaus, law enforcement agencies, insurance companies, the Medical Information Bureau, motor vehicles departments, employers, schools and universities, and state agencies.[11]

Many fear that the Social Security number has become a de facto national identifier.[12] Evan Hendricks noted:

> Not only does the SSN make it easier for large institutions to compare their databases, it allows curious individuals (including private detectives, computer hackers or other strangers you might not want snooping in your private life) to "hop" from database to database and draw out a profile of your buying habits and personal lifestyle.[13]

Whatever the unique identifier that is chosen, the fears expressed by many citizens must be mitigated by establishing a

---

10. *See* H.R. 5464, 102d Cong., 2d Sess. § 2215 (1992) (The Medical and Health Insurance Reform Information Act of 1992); H.R. 200, 103d Cong., 1st Sess. § 321(c)(2)(C) (1993) (Health Care Cost Containment and Reform Act of 1993).

11. *See* OFFICE OF INSPECTOR GEN., DEP'T OF HEALTH AND HUMAN SERVS., THE EXTENT OF USE OF SOCIAL SECURITY NUMBERS 1-5 (1988) (listing the expanded uses of social security numbers under federal law and administrative decisions).

12. *Id.*

13. *Use of Social Security Number as a National Identifier: Hearing Before the Subcomm. on Social Security of the Comm. on Ways and Means*, 102d Cong., 1st Sess. 101, 106 (1991) (testimony of Evan Hendricks, editor of *Privacy Times*).

national privacy policy that explicitly forbids the linking of health care and other information using the SSN. Exceptions for limited, clearly defined purposes such as the development of statistical information in nonidentifiable form may be permitted.[14]

Systematic collection of this highly sensitive personal information can work only in conjunction with a national level privacy policy based on fair information practices. The national policy would replace the current patch work of state laws and would provide the framework for sharing information generated at all levels of the health care system — only a national policy can cover information in interstate commerce.

C. Patient-based Longitudinal Health Records

The growing need for detailed micro-level health data generated by reform efforts is emerging in an environment in which the future vision of health information systems is already undergoing radical change. Although many health records have long existed in automated form, they have traditionally supported specific functions such as the laboratory, pharmacy, or finance department. A fundamental shift to patient-based records is now occurring as part of longer-term efforts toward building national electronic patient-based health information networks.[15]

---

14. For example, the Omnibus Budget Reconciliation Act of 1989, Pub. L. No. 101-239, § 6103(a), 103 Stat. 2106, 2189 (1989) (codified as amended at 42 U.S.C. § 229(a) (Supp. V 1993)), created the Agency for Health Care Policy and Research (AHCPR). It also established a program of research on health care outcomes and procedures, *id.* § 6103(b)(1) (codified at 42 U.S.C. § 132b6-12(a)(1)(Supp. V 1993)), and mandated that:

> the Secretary of Health and Human Services shall report to the Congress on the feasibility of linking research-related data described in section [42 U.S.C. § 132b6-12(d)] with similar data collected or maintained by non-Federal entities and by Federal agencies other than the Department of Health and Human Services (including the Departments of Defense and Veterans Affairs and the Office of Personnel Management).

Id. § 6103(b)(2), 103 Stat. 2106, 2198 (reported at 42 U.S.C. § 132b6-12, Directives).

15. COMMITTEE ON IMPROVING THE PATIENT RECORD, INSTITUTE OF MEDICINE, NAT'L ACADEMY OF SCIENCES, THE COMPUTER-BASED RECORD 31-35 (Richard S. Dick, Elaine B. Steen eds., 1991) While particular groups vary in the specifics of their vision, those focusing on development of automated health care systems, such as the Computer-based Patient Record Institute, Medical Record Institute, and the American National Standards Institute, see a system of several parts emerging in the long run:

- a comprehensive longitudinal computer-based patient record containing all clinical, financial, and research data.

The development of electronic health care networks permitting standardized patient-based information to flow nationwide, and perhaps even worldwide, means that the current privacy protection focus requiring the institution to protect its records must be reconsidered. Our past thinking assumed a paper or automated record that was created and protected by the provider. We may now envision a patient-based record that anyone in the system can call up on the screen.[16] Because *location* has less meaning in an electronic world, many now argue that protecting privacy requires attaching privacy protections to the health record itself, rather than to the institution that generates it.

II. CURRENT LEGISLATIVE PROTECTION OF PRIVACY

Despite these fundamental changes in the health information infrastructure, very little federal legislation of general applicability exists regulating the use and disclosure of personal information by private entities. State law that does exist represents a patchwork of inconsistent and inadequate protection of informational privacy. This section provides a brief history of the protection of health information privacy and examines current legal protections.

A. Contemporary Historical Perspectives on Privacy Protection

Elliot Richardson, the Secretary of Health, Education, and Welfare (HEW) in the early 1970s, mounted a major policy effort on health information privacy. He established an Advisory Committee on Automated Personal Data Systems, which presented its report *Records, Computers, and the Rights of*

•a "national" electronic network for accessing this health record for a variety of purposes such as primary care, insurance payment, peer review, cost containment, public health, and research purposes.

•use of a smart card for purposes ranging from providing health insurance coverage information to providing a conception-to-death record of all health care.

•use of unique patient-specific identifiers in the U.S. and, perhaps, worldwide.

16. John P. Fanning addressed this issue in his U.S. Department of Health and Human Services memorandum. Musings of John Fanning on Legal Controls for Information held in Computerized Systems, Memorandum from John P. Fanning, Senior Health Policy Advisor, Office of Asst. Secretary of Health, U.S. Public Health Service (Apr. 1, 1993) [hereinafter Fanning Memo] (on file with author).

Citizens[17] in 1973. The Committee developed principles of "fair information practices" including personal control of data, no secret record systems, rights of access and correction, and the responsibility of managers for security of data.[18]

A significant outgrowth of that effort was the Privacy Act of 1974,[19] which Congress developed from the principles in the HEW report. The Act covers data collection and maintenance by Federal government agencies, but not by the private sector. Its approach is to set up a comprehensive data management scheme and procedures, rather than strong disclosure prohibitions. It includes some control over the use of the social security number by all government agencies, including those at the state and local levels. In addition, the Privacy Act established the Privacy Protection Study Commission that was time-limited and had no supervisory or regulatory powers. The Commission reviewed the use and disclosure of personal data in a wide variety of fields and produced a report *Personal Privacy in an Information Society*.[20] The report made recommendations in the areas of financial, medical, research, statistical, tax, and government access to records.[21] At the same time, the Nixon administration developed a mechanism for ongoing attention to these issues in the form of the Domestic Council Committee on the Right of Privacy.[22]

The 1977 Privacy Protection Study Commission recommended the enactment of legislation that would regulate certain disclosures of medical records (e.g., direct treatment, health and safety, biomedical or epidemiological research, audit or evaluation, and judicial summons or subpoena). It pre-

---

17. SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973).

18. *Id.* at 41.

19. *See* Gostin, *supra* note 2, (manuscript at 53-5, on file with author) (describing the Federal Privacy Act of 1974 as it relates to health information).

20. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977).

21. *Id.* at 306-07 (recommending guidelines that will preserve the expectation of confidentiality in the medical care relationship).

22. Address of President Nixon (radio broadcast, February 23, 1974) (transcript *in* PUB PAPERS OF RICHARD NIXON 174 (1974)) (establishing a White House committee to examine the collection, storage, and use of personal data in computer retrieval systems, chaired by then Vice President Ford). *See also* THE DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY AND THE COUNCIL OF STATE GOVERNMENTS, PRIVACY, A PUBLIC CONCERN A RESOURCE DOCUMENT (1975).

scribed a series of data protection measures that limited disclosure "to information necessary to accomplish the purpose for which the disclosure is made," required individuals to be informed of disclosures that may be made without their express authorization, and mandated the use of carefully defined and circumscribed forms for required authorizations.[23]

The Privacy Commission delivered its report to the Carter administration which established a privacy initiative and developed bills to implement the recommendations in the report; however, these bills were generally unsuccessful in obtaining passage. Limited financial privacy legislation was enacted, and although medical record privacy legislation was considered at length in both houses of Congress, it failed in a floor vote in the House in December of 1980.[24] The comprehensive bill to address medical record privacy that was presented sought to establish minimum standards for medical care facilities, not individual physicians.[25] The most debatable part of the Federal Privacy of Medical Information Bill was Part C which authorized fourteen separate types of disclosures of medical information without patient authorization.[26] However, most of the disclosures allowed were qualified by language requiring some accounting, reporting, and documentation of the need for disclosures and restrictions on redisclosures. The institution (i.e., hospital or nursing home) also could impose additional requirements for disclosures made without the consent of the patient. Other medical information acts, including the American Medical Association's (AMA) Model Confidentiality of Health Care Information Act[27] and the National Conference of Commissioners on Uniform State Laws' Uniform Health-Care Information Act[28] also list many disclosures without patient authorization.

---

23. PRIVACY PROTECTION STUDY COMM'N, *supra* note 20, at 313-15.

24. *See* 132 CONG. REC. H1625-01 (1986) (noting that despite Congressional agreement that existing legislation inadequately protected medical records, the Privacy Commission's recommendations were not enacted).

25. *See* H.R. Rep. No. 832, 96th Cong., 2d Sess., pt. 1, at 7 (1980) (accompanying H.R. 5935).

26. *Id.* at 8.

27. AMERICAN MEDICAL ASS'N, DEP'T OF STATE LEGISLATION, MODEL CONFIDENTIALITY OF HEALTH CARE INFORMATION ACT § 4(b) (1994) (on file with author).

28. UNIFORM HEALTH-CARE INFORMATION ACT 1985, at § 2-104 (1985).

Although the Carter administration was generally supportive, the American Civil Liberties Union and other organizations were critical of the long list of disclosures of medical information allowed without patient consent.[29] In addition, the AMA and the American Hospital Association (AHA) opposed comprehensive federal legislation for medical privacy arguing that states should handle the matter.[30]

In 1981, the National Association of Insurance Commissioners (NAIC) proposed a model act, the Insurance Information and Privacy Protection Model Act, which fifteen states have adopted.[31] The model bill requires provision of notice of fair insurance information practices,[32] specifies the content of disclosure authorization forms,[33] and regulates access to recorded personal information.[34] The act authorizes separate disclosures without the written consent of the individual, including for disclosures for marketing.[35] While the insurance regulatory official of a state is responsible for monitoring under the act,[36] it is not known whether the model act is proving to be effective in practice.

All the efforts until this time were based upon the assumption that more and more data would be needed and used. Rules were established to insure that collection of systematic health data proceeded without causing undue harm to the individual. The major efforts took a procedural approach and enunciated principles to assure fairness in maintaining and disclosing data. These efforts offered little philosophical basis for making choices whether the collector of information should keep partic-

---

29. *Federal Privacy of Medical Information Act: Hearing on H.R. 5935 Before the Subcomm. on Health of the House of Representatives Comm. on Ways and Means*, 96th Cong., 2d Sess. 37-38 (1980) (statement of the American Civil Liberties Union read by Marcia K. Goin, Chairperson, Committee on Confidentiality, American Psychiatric Association).

30. *Id.* at 56-58, 82-85 (prepared statements of the American Medical Association and American Hospital Association).

31. 4 NATIONAL ASS'N OF INS. COMM'RS. MODEL INSURANCE LAW, REGULATIONS AND GUIDELINES. NAIC Insurance Information and Privacy Protection Model Act, at 670-1, 670-23 to 670-25 (1994).

32. *Id.* § 4.

33. *Id.* § 6.

34. *Id.* § 8.

35. *Id.* § 13(K).

36. *Id.* § 14.

ular records at all or whether an individual should consent to disclosure.[37]

Proposals for computerizing medical records[38] have stimulated attention to privacy hazards. In June 1992, then Secretary of HHS, Louis Sullivan, forwarded a draft bill to Congress that would have mandated the automation of the Medicare claims system and some hospital medical records, required the use of "smart cards" and of the social security number as the unique identifier for health care information, and strengthened privacy protections.[39]

The President's Health Security Act and several other health care reform bills introduced in Congress in 1994 had detailed provisions for the development of a health information infrastructure.[40] In particular, the Fair Health Information Practices Act of 1994, introduced by Representative Condit, provided a comprehensive strategy for protection of health information through the formation of health information trustees.[41] These trustees would fulfill a fiduciary duty to the patient by adopting fair information practices throughout a modern health care system.

C. Current Legal Protection of Health Information Privacy

In Congressional testimony on April 21, 1986, Robert R. Belair summarized the state of health information privacy protection as "very poor" and "unprotective of patient interests."[42] Another commentator concluded that federal and state law "affords meager guidance for establishing a framework for the protection of medical records."[43] A recent U.S. Department of Health and Human Services report concluded that state rules

---

37. Fanning Memo, *supra* note 16.

38. *See supra* notes 5-8 and accompanying text.

39. *See* S. 2878, 102d Cong., 2d Sess. §§ 2211, 2215 (1992).

40. *See, e.g.*, H.R. 3600, 103d Cong., 2d Sess. § 5101 (1994) (Health Security Act); S. 1770, 103d Cong., 1st Sess. § 3308 (1993) (Health Equity and Access Reform Today Act of 1993) (containing general principles that must be considered when developing privacy and confidentiality standards).

41. H.R. 4077, 103d Cong., 2d Sess. (1994).

42. *Information Technologies in the Health Care System: Hearing Before the Subcomm. on Investigations and Oversight of the Comm. on Science and Technology*, 99th Cong., 2d Sess. 141 (1986) (statement of Robert R. Belair).

43. Bernard R. Adams, *Medical Research and Personal Privacy*, 30 VILLANOVA L REV. 1077, 1089 (1985).

superimposed on a federal regulatory framework result in a morass of erratic law, both statutory and judicial.[44]

Perhaps the most often cited problem with the current collection and use of information is the lack of any national-level policy establishing a legal right of medical privacy. More protection exists for credit records and video rental information than exists for sensitive personally identifiable health care information.[45] What protection does exist is in the form of disparate and often conflicting state laws and narrow federal regulations. State privacy laws do exist, but they are not uniform, may not address automation of health information, or may serve as an impediment to automation. In sum, there exists only an inconsistent and usually unenforced web of law that leaves many gaps in protection of privacy.

Although there is an inherent understanding of the need for confidentiality of medical record information, it also should be recognized that the integrity and accuracy of such information is of equal importance. If information used in health care applications is not accurate, at best, it may be useless for intended purposes and, at the extreme, it actually may pose a life-threatening danger. Also, no specific standards that address the need for ready availability of health data exist.

Current privacy and confidentiality protections are a product of federal and state constitutional law, federal and state statutes, and state common law. The Supreme Court held in *Whalen v. Roe*[46] that when states establish reporting requirements, the public health department must have minimal standards for protecting the privacy of sensitive medical information.[47] The doctrine of *Whalen v. Roe*, however, applies only to governmental agencies, not to private parties; it has been rarely

---

44. *See* WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, REPORT, OCTOBER, 1993, App. 4, 3 (1993) (discussing the implementation of identification system to be used for health care services).

45. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681s (1988 & Supp. V 1993) (regulating release of credit reports); Video Privacy Protection Act, 18 U.S.C. § 2711 (1988)(regulating disclosure of videocassette rental records).

46. *Whalen v. Roe*, 429 U.S. 589, 603-04 (1977) (describing the safeguards designed to prevent unauthorized access to computerized records of prescription drugs).

47. Lawrence O. Gostin, *The Future of Public Health Law*, 12 AM. J.L. & MED. 461, 485 (1986).

and inconsistently applied outside the specific facts of that case.[48]

Since the 1970s, more than a dozen states have adopted constitutional amendments designed to protect a variety of privacy interests, including limitations on access to personal information.[49] Although most of the state constitutional provisions only protect against breaches of privacy by governmental agencies, some courts also have applied their guarantees to private parties.[50]

The main protection for informational privacy resides in legislation and the common law. The landmark Federal Privacy Act of 1974 protects citizens from government disclosure of confidential information.[51] Hospitals operated by the federal government and private health care or research institutions maintaining medical records under government contract are subject to its provisions. The Act, however, does not apply to other institutions.[52]

Federal law[53] creates strict rules for maintaining the confidentiality of records of patients treated for drug or alcohol dependency at facilities receiving federal assistance.[54] The protections apply only to specialized substance abuse treatment facilities and to specialized units within general medical facili-

---

48. *See, e.g., J.P. v. DeSanti*, 653 F.2d 1080, 1090-91 (6th Cir. 1981) (holding that constitutional privacy rights do not extend to disclosures of personal information contained in juvenile delinquent social histories); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980) (adopting specific set of criteria for applying constitutional principles of informational privacy). *See also* Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, B.U. L. REV. 133, 146-150 (1991) (reviewing circuit court interpretations of *Whalen*).

49. ROBERT E. SMITH & JAMES S. SULANOWSKI, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 32-37 (1992).

50. *See Soroka v. Dayton Hudson Corp.*, 1 Cal. Rptr. 2d 77, 85 (1991) (construing protection of privacy rights under state constitution more expansively than rights protected by the U.S. Constitution); *Rasmussen v. South Florida Blood Serv.*, 500 So.2d 533, 536-37 (Fla. 1987) (citing the state constitution in holding that the disclosure of blood donors implicated constitutionally protected privacy interests).

51. 5 U.S.C. § 552a (1988 & Supp. V 1993).

52. *See* 5 U.S.C. § 552(f) (West Supp. 1994) (defining "agency" for purposes of 5 U.S.C. § 552).

53. 42 U.S.C. § 290dd-2 (Supp. V 1993); 42 C.F.R. § 2.1-2.67 (1993).

54. Federal assistance includes tax-exempt status. 42 C.F.R. § 2.12(b)(4) (1994). *See generally* NATIONAL INST. ON DRUG ABUSE, U.S. DEP'T OF HEALTH AND HUMAN SERVS., LEGAL OPINIONS ON THE CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS 1975-1978 (providing legal opinions by the OIG interpreting the federal alcohol and drug abuse confidentiality statutes).

ties, but not to substance abuse information in general medical records.[55]

Many states have privacy protection contained in medical and other professional practice acts, hospital, and other institutional licensure laws and, in some cases, comprehensive medical information statutes. These statutory schemes also contain many important gaps in coverage. Many state medical records statutes, for example, contemplate or require maintenance of manual patient records so the protection afforded to automated records is uncertain.[56] In addition, in most states there is little or no regulation of the informational practices of insurers. Only fifteen states have adopted model privacy legislation drafted by the NAIC.[57]

Other state laws offer a patchwork of privacy protection that is often disease-specific. For example, most states protect information regarding HIV infection or AIDS.[58] However, many of these states allow or even require disclosure in so many situations that the privacy rule itself becomes virtually meaningless. Many state sexually transmitted disease statutes contain strong protections of confidentiality, but communicable disease or tuberculosis statutes contain weak protections or none at all.[59]

Most states recognize a common law duty of confidentiality applying to certain health care professionals. Thus, if a patient discloses personal information to a health care professional believing that it is private, the professional may be liable

---

55. *See* 42 C.F.R. § 2.11 (1994) (defining programs covered under the statute).

56. *See* Deborah K. Fulton, *Legal Problems Arising in the Automation of Medical Records*, 8 TOPICS IN HEALTH REC. MGMT. 73, 74 (1987) (discussing the requirement that medical records fulfill licensing and other regulatory mandates that computerized records may not be able to meet).

57. NATIONAL ASS'N OF INS. COMM'RS, *supra* note 31, at 670-23 to 670-25.

58. 1 MONA ROWE & BETHANY BRIDGHAM, EXECUTIVE SUMMARY AND ANALYSIS: LAWS GOVERNING CONFIDENTIALITY OF HIV-RELATED INFORMATION: 1983 TO 1988, at I-4 (1989); *see also* 2 MONA ROWE & BETHANY BRIDGHAM, INDIVIDUAL STATE SUMMARIES: LAWS GOVERNING CONFIDENTIALITY OF HIV-RELATED INFORMATION 1983-1988 (1989) (providing a state-by-state analysis of HIV-related confidentiality protections).

59. Gostin, *supra* note 47, at 485-86 (describing state confidentiality protection for sexually transmitted diseases); Lawrence O. Gostin, *Controlling the Resurgent Tuberculosis Epidemic: A 50-State Survey of TB Statutes and Proposals for Reform*, 269 JAMA 255, 260 (1993) (describing the limitations of state statutes protecting tuberculosis patients).

for disclosure without the patient's consent.[60] While common law protections of confidentiality probably provide the most consistent safeguards, significant gaps exist in legal duties. For example, in many states, the legal duties of physicians to safeguard patient confidences do not extend to other health care professionals, researchers, or health care institutions, even though the risk of harm from disclosure may be as great or greater.[61]

For several important reasons, continued reliance upon current legal safeguards is incompatible with the policy objectives of an integrated national health care system.[62] A state-by-state approach to regulation of medical information does not reflect the realities of modern health care finance and delivery. 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 differing legal requirements, for a wide variety of purposes ranging from medical consultation and research collaboration to governmental monitoring for quality.

Further, the physical location of health information is no longer a relevant consideration for development of privacy policies. Databases containing huge quantities of health information provide the potential for immediate access by a variety of eligible users in remote locations. Thus, state laws that attempt to regulate information physically contained in a particular state are anachronistic vestiges of a pre-electronic era.

The prospects for resolving privacy problems through the enactment of model or uniform laws in every state is exceedingly small. The National Conference of Commissioners on Uniform State Laws developed the Uniform Health-Care In-

---

60. *See, e.g., Humphers v. First Interstate Bank of Oregon*, 696 P.2d 527, 535-36 (Or. 1985) (en banc) (holding a physician liable for breach of confidential relationship).

61. *See People v. Baker*, 288 N.W.2d 430, 431 (Mich. Ct. App. 1979) (refusing to extend physician-patient privilege to optometrist); *Quarles v. Sullivan*, 389 S.W. 2d 249, 251 (Tenn. 1964) (refusing to imply a contract of confidentiality between company doctor and an employee examined by him); Wendy Parmet, Note, *Public Health Protection and the Privacy of Medical Records*, HARV. C.R.-C.L. L. REV. 265, 274 (1981) (noting that physicians provide less than 5% of American health care).

62. WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 8, at app. D (1993) (discussing confidentiality, privacy, and security concerns with computer-based patient records).

formation Act in 1985, but only two states, Montana and Washington, have enacted it.[63]

The absence of uniform privacy and confidentiality protection applicable throughout the country imposes hardships on most everyone. Health care institutions, insurance companies, and self-insured employers who transmit health information through interstate commerce often do so without clear guidance regarding which state's laws govern or which state's courts have proper jurisdiction to resolve disputes that may arise. Without the ability to know and to rely upon uniform privacy regulations, patients may lack the basis for meaningful consent to disclosure of information. Lack of uniformity of privacy protections may adversely affect the integrity of health data and the quality of care itself by undermining efforts to automate health records.

These detriments of state-by-state privacy protections would only be magnified in a health care system where patients would be entitled to coverage anywhere they live in the country and where information for monitoring quality and cost-effectiveness would be collected nationally. Consequently, many persuasive reasons exist to adopt a uniform federal privacy policy that transcends state borders.

III. THE ETHICAL FRAMEWORK FOR PRIVACY

In health care settings, a balance must be struck between the rights and interests of individual patients and the potentially competing interests of other individuals, families, groups, and society generally. The nature and degree of protection that should be accorded to the individual's interests in privacy and confidentiality are among the most significant questions to be addressed in the process of health care reform. The task is to secure an adequate measure of respect for the privacy and autonomy of the individual consistent with societal needs for an efficient system of health care finance and delivery, an adequate and reliable informational basis for health care planning, and an enhanced capability for promoting and protecting the public's health.

---

63. *See* MONT. CODE ANN. § 50-16-501-50-16-553 (1993); WASH REV. CODE ANN. §§ 70.02.005-70.02.904 (West 1991).

The potential harm to individual interests from disclosure of personal medical or health information, as well as a strong presumption in our society for respecting autonomy (the right of the individual to retain control over aspects of his or her own person) provide powerful arguments for restricting the access others may have to such information. However, the informational requirements for realizing legitimate societal goals of health care reform may necessitate that more rather than less personal information is generated, collected, and made available to designated others for a variety of treatment, research, and policy planning purposes.

A. Definitions of Privacy and Confidentiality

PRIVACY: A preliminary step in the analysis of how an individual's interests in privacy ought to be balanced against other social goals is definitional. Legal, philosophical, social science, and medical literatures abound with many different, competing theories of privacy; no definition is likely to command universal assent.

An influential definition attributed to Samuel Warren and Louis Brandeis holds that privacy consists in being let alone.[64] Critics object that this definition is too broad, and that there are innumerable ways of being interfered with, or not being let alone, that have nothing to do with privacy.[65] Consequentially, theorists have sought to refine privacy definitions to isolate what is unique about privacy and what constitutes its loss, and to reflect better the multiple dimensions of privacy.

Among the most prominent of such attempts are those which define privacy as a condition of limited or restricted accessibility to some aspect of the person.[66] However, to remain inaccessible to others in some respect is not necessarily to be inaccessible in all respects. Anita Allen usefully distinguishes

---

64. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 75, 75 (Ferdinand D. Schoeman ed., 1984). *But see* Ruth Gavison, *Privacy and the Limits of Law, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 346, 357 (Ferdinand D. Schoeman ed., 1984).

65. *See, e.g.*, W. A. Parent, *Privacy, Morality and the Law*, 12 PHIL. & PUB. AFF 269, 272 (1983).

66. *See generally* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1987) (surveying limited access or restricted access definitions).

among three types of inaccessibility — dispositional, physical, and informational:

> [P]rivacy is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others. To say that a person possesses or enjoys privacy is to say that, in some respect and to some extent, the person (or the person's mental state, or information about the person) is beyond the range of others' five senses and any devices that can enhance, reveal, trace, or record human conduct, thought, belief or emotion.[67]

Other definitions similarly emphasize the many possible aspects of a person for which increased access might be counted as a particular kind of privacy loss. For example, Ruth Gavison's definition includes limited access in the sense of solitude, secrecy, and anonymity.[68]

Such multi-dimensional, limited-access definitions mark useful distinctions among the various types of privacy losses that individuals may experience. Moreover, they illuminate the extent to which a loss of privacy in one respect often can result in a loss of privacy in another. For example, the involuntary testing of a patient for a genetic condition or HIV infection involves a loss of physical privacy in the process of drawing the patient's blood, as well as a loss of informational privacy when the results are analyzed in the laboratory and recorded in a medical system.

The blood test example also reveals a fourth sense of privacy widely familiar in both moral and legal theory. Many will count the involuntary testing itself as involving a loss of what has come to be known as decisional privacy.[69] Critics of decisional privacy complain that this extension of the concept rests upon a confusion. They argue that the fundamental interests at stake are not privacy interests but liberty interests, and that what is morally relevant is the loss of liberty or deprivation of autonomy.[70]

Although the dimension of privacy most centrally at stake in the health care system is informational privacy, other mor-

---

67. *Id.* at 15.

68. GAVISON, *supra* note 64, at 354.

69. Anita L. Allen, *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*, 56 U. CIN. L. REV. 461, 461 (1987).

70. *See* Parent, *supra* note 65, at 273-74.

ally significant issues having to do with the individual's ability to retain autonomous decision-making authority over important aspects of his or her life are never far from that central concern.

CONFIDENTIALITY: A closely related issue in the general discussions of informational privacy is that of confidentiality. Confidentiality is a characteristic of a relationship, such as that of a physician and his or her patient. Equally, confidentiality is a property of certain kinds of information, such that by the information's very nature it ought not to be revealed to others without the person's permission.

In American law, under many circumstances, certain information disclosed by an individual to a physician in the context of a physician-patient relationship is protected from further disclosure to others without a bona fide need to know. The relationship is a confidential one; the information is confidential in nature; and the physician is under a legal duty of confidentiality.

Even in such a relatively straightforward statement of the law, however, there are many thorny issues regarding confidentiality. First, surely not all information learned by a physician is the proper subject of such a duty. Arguably, only information that relates to the patient's health status or other highly sensitive or personal matters that the patient would not have disclosed if the patient had not sought medical treatment would qualify as confidential.

Second, there are substantial ambiguities about what constitutes a physician-patient relationship. Without a threshold determination that such a relationship exists, it is unclear, as a legal matter at least, that the physician is under any duty of confidentiality. The relationship between company physicians and the employees they examine is a familiar instance of this kind of controversy in the law.[71]

Third, although traditional medical ethical norms, dating as far back as the Oath of Hippocrates, reflect a strong commitment to preserving the secrets of the patient, traditional

---

71. *See, e.g.*, Bratt v. I.B.M. Corp., 467 N.E.2d 126, 137, nn. 21-22 (Mass. 1984) (noting the tension between the general rule that when an employer retains a physician to examine employees, no physician-patient relationship exists between the employee and the physician, and the implicit rules evident in numerous statutes that patients have a recognized interest in the confidentiality of personal information disclosed to a physician).

common law in the U.S. is more equivocal. Common law rules often permit disclosure of confidential information in the course of litigation or to protect third parties. Thus, particular information disclosed in the context of certain professional relationships is best understood now as presumptively confidential, or such as to establish a *pro tanto* duty not to disclose without the express or implied consent of the patient.

B. Ethical Justifications for Privacy and Confidentiality Protection

THE MORAL IMPORTANCE OF PRIVACY: The literature on privacy abounds with accounts of the moral justifications for rules of privacy. The different kinds or forms of privacy — seclusion, limited access, and informational privacy — highlight different justifications and moral values. Still, it is possible to sketch the general moral considerations at stake in respecting privacy.

One standard account holds that the primary justification for respecting privacy resides in the principle of respect for autonomy. To respect the privacy of others is to respect their autonomous wishes not to be accessed in some respect — not to be observed or have information about themselves made available to others. Joel Feinberg has observed that historically the language of autonomy has functioned as a political metaphor for a domain or territory in which a state is sovereign.[72] Personal autonomy carries over the idea of a region of sovereignty for the self and a right to protect it — an idea closely linked to the ideas of privacy and the right to privacy. The link between privacy and autonomy is thus straightforward — respecting privacy is one way or form of respecting autonomy.

This straightforward link between privacy and autonomy does not, however, exhaust the relationship between these two concepts. Respecting privacy is an important means of fostering and developing a sense of self, of personhood, and of personal autonomy. Indeed, without some level of privacy, it is dif-

---

72. Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?*, 58 NOTRE DAME L. REV. 445, 452 (1983) ("The politically independent state is said to be sovereign over its own territory. Personal autonomy similarly involves the idea of having domain or territory in which the self is sovereign. But whereas international conventions and treaties have long since defined the idea of 'national territory' with some precision, the 'boundaries' of the personal domain are entirely obscure and controversial.").

ficult to imagine how individuals can formulate autonomous preferences or, more basically, develop the capacity to be self-governing. Certain conditions of privacy are necessary for the development or at least the fostering of personhood and personal autonomy. Thus, privacy is of instrumental value where it promotes personhood, autonomy, or self-governance.

Personhood and personal autonomy are not, however, the only or even necessarily the most morally significant ends promoted by privacy. Privacy enhances the development and maintenance of intimate human relationships — relations of trust, friendship, and love. It is arguably one of the defining characteristics of intimate relationships that they involve the sharing — freely given — of private information, spaces, and acts. In an intimate relationship, we allow another to enter the otherwise private sphere of our lives. If privacy is not cherished and respected, both the capacity for, and meaning of, intimacy in human relationships are clearly diminished. Indeed, as Charles Fried has argued, "privacy is . . . necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather, without privacy they are simply inconceivable."[73]

Additionally, information frequently is viewed as a resource, the possession of which by others enables them to exercise power over individuals.[74] This raises the possibility of exploitation and the consequential loss of psychological, social, and economic well-being.

We need not here resolve which is the more foundational moral justification for respecting privacy — the formation of intimate relationships, respect for autonomy, or the development of personhood and capacity for autonomous expression. The central point here is that privacy's moral value is in the main derivative and based on a complex of moral commitments and concerns.

RULES OF MEDICAL CONFIDENTIALITY: At least five kinds of moral arguments may be used to justify rules of confidentiality in the medical context. First, rules of medical confidentiality should be respected as instances of general obligations to re-

73. Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).
74. Parent, *supra* note 65, at 276.

spect informational privacy. Second, medical confidentiality must be respected because of the special moral character of the physician-patient relationship. That is, confidentiality is intrinsic to the very nature of this relationship, characterized as it is (or should be) by trust and intimacy. Third, medical confidentiality should be respected because there is at least an implicit and sometimes explicit promise of confidentiality embedded in the institution of medical care, and it is wrong to break a promise. Fourth, rules of medical confidentiality should be respected because these rules are necessary to bring about good to patients and to society; without this assurance of confidentiality, people would not share medically relevant information. Finally, rules of medical confidentiality should be respected because they are necessary to prevent patients from the harm that could reasonably befall them if information collected in the course of treatment became publicly available.

D. Potential Harms Created By Loss of Informational Privacy

The ethical justifications for privacy protections and rules of confidentiality point to a variety of underlying harms that may result from unwanted disclosures of personal medical or health status information. These harms can be classified as intrinsic and consequential moral harms.

Intrinsic moral harms are those that result from the mere fact of an unwanted or unjustified disclosure of personal information. Many moral views at least recognize the desirability of protecting individuals against insult to dignity and the lack of respect for the person evidenced by such disclosures.

Consequential harms are those that result from a loss of privacy, and they matter morally regardless of whether the loss of privacy is a consequence of an intentional, negligent, or perfectly innocent action of another. The morally significant feature of such losses of privacy lie in the actual harm that is caused.

Consequential harms can affect a person's economic interests. These include the potential loss of employment or employability or loss of insurance or insurability. Often the loss of insurance and employment (or insurability and employability) go hand-in-hand when, for example, the only affordable insurance is through employment, or the most effective way employ-

ers have to contain the costs of production is to hold down employee benefit costs by excluding from the workforce those costly to insure. Another economic interest at risk of harm from invasion of privacy is loss of housing opportunities, especially for those having stigmatizing conditions such as HIV infection, tuberculosis, mental illness, or a history of drug or alcohol abuse.

A second category of harm involves social or psychological dimensions. Disclosure of some conditions can be stigmatizing and can cause embarrassment, social isolation, and the loss of self-esteem. These risks are especially great when the perceived causes of the medical condition or illness include the use of illegal drugs, socially disfavored forms of sexual expression, or other behavior not widely socially approved.

Moreover, stigmatization may be a consequence of such disclosures in some instances even when the potential causes do not involve any despised choices or behavior on the part of the affected individual. Family members, neighbors, and work associates may withdraw social support from those learned to have certain conditions or diseases, especially if such conditions involve mental or emotional instability or physical or behavioral attributes that some individuals find uncomfortable to observe. Indeed, such stigmatization may occur even toward those who do not currently manifest symptoms of a disease.

E. When Privacy Is Not the Paramount Consideration

Although privacy is important, it is not always unambiguously a positive value. Some states or conditions of privacy are undesirable or morally wrong, as when seclusion brings loneliness or isolation, and secrecy conceals wrongdoing or harms others. Even when privacy is unambiguously a good, it is not always paramount in conflicts with other cherished values. Privacy interests can be outweighed by competing moral considerations of greater value in the circumstance. For example, there may be a need to access an individual's personal health information in order to prevent harm to an identifiable other party, or to benefit the person who is the subject of the information,

or to benefit another person.[75] Alternatively, access to the information may be needed in order to further the legitimate and valued social interests of all citizens in such matters as public accountability, monitoring, and evaluation of the health care system, efficiency in the delivery of care, scientific advance and medical knowledge, and the public's health.

IV. FAIR INFORMATION PRACTICES

Concern for protecting personal privacy is a leading issue in all Western industrial societies. Legislators have responded to these concerns by enacting protective laws. Principles of fair information practices, although stated somewhat differently from country-to-country, serves as the basis for these laws. In the U.S., traditional fair information practice principles are the foundation for the Privacy Act of 1974 which applies to federal records. These practices stipulate that individuals about whom data are collected have the right to know about and approve the uses to which data are put, that no secret data systems are permitted to exist, and that individuals have the right to review and to correct data about themselves.

Following these principles requires that: (i) information should be collected only to the extent necessary to carry out the purpose for which the information is collected; (ii) information collected for one purpose should not be used for another purpose without the individual's informed consent; (iii) information should be disposed of when no longer necessary to carry out the purpose for which it was collected; (iv) methods to ensure accuracy, reliability, relevance, completeness, and timeliness of information should be instituted; (v) individuals should be notified (in advance of the collection of information) whether the furnishing of information is mandatory or voluntary, what recordkeeping practices exist, and what the uses will be made of the information; and (vi) individuals should be permitted to inspect and correct information concerning themselves.

---

75. *See, e.g., Tarasoff v. Regents of the Univ. of California*, 551 P.2d 334, 343 (Cal. 1976) (imposing upon psychiatrist an affirmative duty to warn third parties to prevent foreseeable, unreasonable risk of harm).

A. Informed Consent

If a goal of privacy protection is to ensure the right of individuals to exercise control over information about themselves, then procedures for ensuring informed consent have to be expanded, enhanced, and regularized.[76] Individuals have a right to learn what will happen with their personal information, even if many of the disclosures are mandatory. The key elements of informed consent are thorough disclosure, comprehension of the information, voluntariness in acting, competence to act, and consent to the action.[77]

Creative and responsive informed consent procedures can readily be built into software used in hospitals or physicians' offices. The software could automatically remind health care providers of the need to renew an informed consent statement for a particular patient after the lapse of an agreed-upon time. Patients should be reminded, perhaps once a year, of how their personal data are being used for any purpose beyond direct care and billing.

B. Use of Data for Intended Purposes

One of the core fair information practices is that personal data should be used only for the purpose for which they were collected. The Organisation for Economic Co-operation and Development's influential 1981 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* specify that the purpose for which personal data are collected should be specified not later than at the time of data collection. The subsequent use should be limited to the fulfillment of those purposes or compatible purposes. Subsequent uses should be specified on each occasion of change of purpose. Such data cannot be otherwise used without the consent of the data subject or without legal authority.[78]

---

76. *See generally* FAY A. ROZOVSKY, CONSENT TO TREATMENT: A PRACTICAL GUIDE (2d ed., 1990) (discussing procedural protections for informed consent).

77. Tom L. Beauchamp, *Informed Consent, in* MEDICAL ETHICS 173, 180 (Robert M. Veatch ed., 1989).

78. ORGANISATION FOR ECONOMIC COOPERATION AND DEV., GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 10 (1981).

C. Access to Records

The principle of granting all individuals full access to their medical and health records has not received appropriate legal or practical attention. Many persons do not enjoy such access and the empowerment that would come from knowing what is being written about them. Some states do not provide a statutory right of access to a patient's own medical record.[79] It is possible even to imagine, over time, a trend toward the use of "plain English" in medical record keeping, such as has occurred in U.S. credit reporting.

D. Self-regulation and Training of Staff

All organizations and offices that collect health information, including hospitals and health insurance companies, must produce their own information codes within the framework of fair information practices that govern their behavior. Preparation of a privacy protection policy is an excellent method of requiring specialized groups to consult their own self-interest, to report on their own good practices, and to formulate reasonable solutions to outstanding problems. Such efforts at self-regulation can result in pamphlets and public notices used to inform the general public better about the privacy code in place and to assuage consumer concerns in specific settings. Ideally, for example, a hospital's Privacy Protection Committee should treat such matters on an ongoing basis.

Staff in institutions and organizations must be trained and retrained; detailed manuals of appropriate procedures must be developed; and monitoring and auditing of compliance with stipulated norms must be in place.

V. SECURITY OF HEALTH INFORMATION SYSTEMS

The National Research Council (NRC) states "*[t]he nation needs computer technology that supports substantially in-*

79. *But see* Terri F. Arnold, Note, *Let Technology Counteract Technology: Protecting the Medical Record in the Computer Age*, 15 HASTINGS COMM. & ENT. L.J. 455, 471 (1993) (noting that many states have affirmed patient access rights).

creased safety, reliability, and, in particular, security."[80] The NRC further defines security as:

> protection against unwanted disclosure, modification, or destruction of data in a system and also the safeguarding of systems themselves. Security, safety, and reliability together are elements of system trustworthiness — which inspires the confidence that a system will do what it is expected to do.[81]

As automated health care records systems increasingly contain standardized health care information capable of being transmitted nationwide, and perhaps worldwide, over electronic networks, "society becomes more vulnerable to poor systems design, accidents that disable systems, and attacks on computer systems."[82] Opportunities for using electronic health care networks also may be lost if there is serious mistrust of their safety.

Establishing appropriate security standards can, within the proper legislative framework, both strengthen patient privacy and confidentiality and assure that information is available to improve the quality and efficiency of health care services. With existing paper systems, information requests often result in the release of data that are not pertinent to the current request as total documents are photocopied and/or faxed to users. With computerized systems, tailored selection of data items from an individual health record easily makes it possible to share only the information that is necessary to the inquiry at hand. With the establishment of appropriate access requirements, more accurate, reliable, and cost-efficient protection of health care information can be achieved than with non-automated systems.

Automation makes it possible to maintain detailed records of access to information or audit trails that were simply not possible or practical in non-automated systems. Computers watch computers, sometimes on a keystroke-by-keystroke basis, and produce logs that supervisors and security officers can consult when individuals complain or a record of activity on a file or from a specific terminal or operator raises suspicions of unauthorized behavior. Thus, security and data protection officers

---

80. SYSTEM SECURITY STUDY COMM., NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 2 (1991) (emphasis in original).

81. *Id.*

82. *Id.* at 1.

might identify and question patterns of staff browsing in patients' records.[83]

At the same time, computers make the anonymous exploring of data an antiseptic process. Computerization makes files that were difficult to use easier to access and thus increases the range of secondary uses made of the data. A single breach of security can result in a very large amount of information about a lot of persons being disclosed. Computerization also makes it easier to link information from many sources together increasing the potential for undue intrusiveness into people's records and lives. Individuals find it difficult to understand where information about them resides and how that information has been linked or used. Computerization can make it extremely difficult to control effectively the redisclosure of information. Records can be easily transmitted across state lines, making it difficult for any state to offer reasonable protections.

Although making a computer system completely secure is not feasible, much can be done to protect records. With careful planning and use of technology, it should be possible not only to address current privacy and security concerns for health care information, but in some ways actually to improve the degree of protection. At the same time, technological advances in electronic systems are proceeding at an accelerated pace, and more sophisticated systems will soon replace today's state-of-the-art systems.

Data protection policies, if they are to be effective in this rapidly changing environment, must not be tied to specific systems and system capabilities, but rather must establish privacy protection guidelines that define system goals but do not specify how these goals will be reached. These protections will be most effective if privacy is addressed directly at the outset in developing electronic systems. They should guarantee that only those with authorized access can access records for authorized purposes at authorized times. Because computer technology is rapidly evolving, ongoing research ensures that these advances

---

83. *See* JO ANNE C. BRUCE, PRIVACY AND CONFIDENTIALITY OF HEALTH CARE INFORMATION 29-71 (1988) (discussing safeguards to confidentiality through the use of countermeasures and internal audits including confidentiality training, identification badges, requisition systems, and document destruction programs); Arnold, *supra* note 79, at 490 (recommending that courts consider whether information is adequately protected by system tracking and detection).

do not erode security practices. There also will be a need for oversight and management structures promoting the development and proper use of system security principles in the development and implementation of health care data systems.

Effective security protection for health care information will require use of technology that most computer systems and networks do not regularly use today. While this technology exists and has been proven effective and affordable, it is not widely used because it would have to be retrofitted to existing systems or because of perceived costs or inconvenience. A continuing concern has been the acceptability of computer security to health professionals if they perceive that security slows down the flow of information needed for providing health care. These concerns are valid, particularly in emergency situations where seconds count or where the patient is unable to supply the necessary information.

The steps identified by the NRC as necessary for achieving greater computer security and trustworthiness are as applicable to health computer systems as to those serving other purposes. These steps include promulgating a comprehensive set of "Generally Accepted System Security Principles" that would provide a clear statement of essential security features, assurances, and practices.[84] Among the major elements of these principles are quality control, access control on code as well as data, user identification and authentication, protection of executable code, security logging, a security administrator, data encryption, operational support tools to assist in verifying the security state of the system, independent audits of the system, and hazard analysis. Levels of access also can be established recognizing the varying degrees of security required for differing kinds of information.

Threats to confidentiality can emerge from outside an organization as well as among an institution's own personnel, and the security system should be designed to address each type of threat. Regular security checks should be conducted and recorded. In addition to impeding unauthorized access to health information, it is also important to establish that security policies for individuals and organizations who gain legitimate access to patient records through networking, computer sharing,

84. SYSTEM SECURITY STUDY COMM., *supra* note 80, at 27.

and/or outside computer services contracts. Most breaches of security that now occur are the result of "insider" action. Organizations can use routine institutional review and monitoring to evaluate appropriateness of access and security measures. Employers should institute training programs so that employees are fully aware of their responsibilities and the actions required of them in performing their jobs.

Currently, the majority of standards in the U.S. are developed through a voluntary consensus process with participation from both the public and private sectors. Within the federal government, the Omnibus Budget Reconciliation Act of 1989 assigned the Agency for Health Care Policy and Research (AHCPR) responsibility for developing automated medical record standards.[85]

VI. NEEDED ACTIONS

The provision of adequate privacy and security protection measures for health information should be an integral part of the development of a modern health care system. The following recommended actions are based on analysis done in the course of the work of the Health Information and Privacy Committee of the President's Task Force on Health Care Reform.

Recommendation A

Establish, through preemptive federal legislation, a national privacy framework covering all health records that is based upon the Code of Fair Information Practices and incorporates guidelines for informed consent.

No federal level legislation establishing the right of privacy for private sector medical or health care information exists. Current state and local laws are inconsistent and potentially conflicting. A more uniform national standard for privacy and confidentiality would simplify compliance for organizations that operate nationwide and protect information that is increasingly crossing state borders. It also would provide protection for data that are linked or potentially linked to other data systems. More uniform standards would make it easier for patients to

85. *See supra* note 14.

have a clear understanding of how information about them is protected.

The legal framework should establish comprehensive, national level privacy and confidentiality rights for individually identifiable health care information. This national policy would:

(1) be applied to all information whether it is part of a modern health care system or exists outside of it and to all types of health care information, regardless of form (electronic or paper), location (storage, transit, archive), or user/holder (government, provider, private organization);

(2) protect all individually identifiable health care information equally, since different individuals will have different perceptions of what should be considered sensitive; and

(3) establish enforceable and meaningful mechanisms and penalties to ensure compliance and define implementation responsibilities for policy setting, administration, monitoring, enforcement, and standards setting.

Privacy and confidentiality protections should be established for all records whether they exist within a modern health care system or outside it. Both medical records that document the relationship between the physician and patient as well as health records collected about and maintained on individuals outside traditional health care settings must be protected. Records containing substantial health information are developed and maintained by such diverse groups as educators, employers, and law enforcement agencies in the form of administrative and financial files. In order to protect the privacy and confidentiality of the individual, it also is necessary to protect health information in whatever form (paper or electronic) it is maintained.

Traditionally, privacy protection includes restrictions on the disclosure of information without the individual's consent. However, some consent forms are not comprehensible or the individual may be under stress when he or she is asked to complete the consent form, or he or she may give consent under pressure in order to receive some needed service. Therefore, to protect individually identifiable information, the disclosure of information to certain individuals and organizations should take place only with the explicit, voluntary consent of the individual after receiving reliable and clear information about the disclosure. Consent forms for the release of information should be limited in time, describe the type of information to be re-

leased, and provide the purposes for which it is to be released. Consumers should be given an opportunity to define material that they consider to be especially sensitive and for which explicit specific, additional consent for release of information is required.

Information that has no personal identifiers and that cannot be linked to identifiable persons should be available to legitimate researchers without the explicit consent of the individual, subject to approval by an institutional review board or the analogous policy-making board in a modern health care system. These review boards should have explicit guidelines to recognize and prevent demographic information from unintentionally identifying individuals.

Recommendation B

Establish a system of universal identifiers for the health care system.

Unique identifiers are needed to help ensure accuracy of information and efficient operation of the health care system. Such identifiers, however, should not become a risk to the privacy of the individual. Although the Social Security Number (SSN) is the most obvious candidate for a health care identifier, there are serious concerns about the privacy implications in its use. The SSN could make it possible to link health and other information about the individual both within and outside the health care system, and there are some technical problems with the numbers, including validation of accuracy, that would need to be overcome at significant cost prior to its use in a modern health care system.

Recommendation C

Establish a Data Protection and Security Panel(s) for overseeing and managing privacy policy and confidentiality matters and violations and security. While the National Data Protection and Security Panel(s) should play the major policy setting role, states and other regulatory authorities, and health plans also must be active partners in this process.

Establishing a Data Protection and Security Panel(s) will fill a major gap in the privacy and security framework in the U.S. Since 1974, many have proposed the creation of a privacy

protection entity.[86] This panel's responsibilities with respect to the *privacy and confidentiality* of health care information should include:

(1) monitoring and evaluating the implementation of any statutes and regulations enacted through health care reform, and the authority to formally participate in any administrative proceedings or processes having a material effect on the protection of personal privacy, either as a result of governmental or private sector actions or as a result of governmental regulation;

(2) conducting research and studies, investigating areas of privacy concern, and supplementing other mechanisms in the health care system through which citizens question the propriety of information collected and used;

(3) issuing guidelines that must be followed by participants in the health care system in implementing the requirements of privacy statutes (these guidelines may deal with procedural matters and with determinations of what information must be available to individuals or the public;

(4) advising the President and the Congress, government agencies, states, and other members of the health care reform system regarding the privacy implications of statutes or regulations;

(5) supporting the development of consent forms governing the disclosure and redisclosure of information; and

(6) promoting awareness among consumers about their privacy rights as well as the importance of using their health care records for societal purposes such as fostering the advancement of medical research.

This panel's responsibilities with respect to *security* of health care information systems should include:

(1) requiring that security standards be implemented in all health care information systems and establishing penalties for failure to do so;

(2) creating incentives for timely completion of security standards development;

(3) funding pilot projects that demonstrate the technology required for implementing security standards and sharing information in the health care setting;

---

86. *See supra* notes 19-41 and accompanying text.

(4) working with standards development organizations and involved Federal agencies to determine security requirements, and, on the basis of these requirements, setting security standards development priorities; and
(5) working with the health provider community to foster development of security standards responsive to their goals of providing effective medical care.

Recommendation D

Establish a comprehensive program fostering privacy and security education and awareness among all members of the health care system including the consumers of these health care services about whom information is being collected.

Unless those involved in the health care system are aware of their rights and responsibilities, established protections will have limited impact. The Data Protection and Security Panel(s) should play a leadership role in fostering the development and implementation of orientation and training programs for personnel with access to health care information as well as supporting the development of programs for fostering consumer awareness about their rights concerning the development and redisclosure of information about them.

Threats to privacy often arise within organizations. Violations of privacy and confidentially may result from casual or inadvertent disclosure or deliberate disclosure for financial or personal gain. Training programs can be important mechanisms for informing employees of their responsibilities and of the penalties for misconduct. They can help to inculcate respect for individual rights. Operating manuals, monitoring of staff performance, and routine review of audit trails also will contribute to controls on unauthorized release of health care information.

Before establishing any health care information system, there should be public notice of the contents, uses, and privacy impacts of the system, as well as the right for interested groups and individuals to comment on the proposed system to relevant authorities. Handbooks describing patient rights concerning records maintained about them should be distributed by regulatory authorities and health plans. To protect individual rights, individuals have the right to expect, and the system has the obligation to provide, assurances that personal records are as

accurate, timely, and complete as the uses to which they are being put require. They also have the right to know how these records are routinely used and to agree to those uses.

CONCLUSION

Individuals have the right to expect, and the health care system has the obligation to provide, assurances that personal records are accurate, timely and complete, and that records will be confidential and maintained in a secure system. The success of the health care system depends in large part on the integrity of information and the confidence of the public that private information will be vigorously protected.