Introduction, Summary, and Options

1

Computerization of health care information, while offering new opportunities to improve and streamline the health care delivery system, also presents new challenges to individual privacy interests in personal health care data. Technical capabilities to secure and maintain confidentiality in data must work in tandem with legislation to preserve those privacy interests while making appropriate information available for approved uses.

BACKGROUND AND STUDY APPROACH

Previously, the Office of Technology Assessment has explored the need to protect the confidentiality and integrity of data and information that is processed and transmitted using communications and computer technology.[1] OTA's objectives for this study were to:

Health information and the medical record include sensitive personal information that reveals some of the most intimate aspects of an individual's life.

[1] In 1986, the Senate Committee on Governmental Affairs and the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties and the Administration of Justice, requested that OTA examine the impact of new technological applications, such as the computerized matching of two or more sets of records, networking of computerized record systems, and computer-based profiles on individuals for balancing the privacy of citizens with management efficiency and law enforcement. In response to that request, OTA prepared the report *Electronic Record System and Individual Privacy, OTA-CIT-296* (Washington, DC: U.S. Government Printing Office, June 1986). That report found that privacy is a significant and enduring value held by Americans, and that the courts have not determined adequate constitutional principles of information privacy. It concluded that the advances in information technology enable Federal agencies to process and manipulate information with great speed.

A 1987 Office of Technology Assessment report, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-31O* (Washington, DC: U.S. Government Printing Office, October 1987), examined the vulnerability of communications and computer systems, and technology for safeguarding information. The report recognized that government agencies, the private sector, and individuals are using sophisticated communications and computer technology to store, process, and transmit information that needs to be protected.

- examine the technology enabling the computerization and networking of medical information,
- identify privacy issues arising from computerization,
- examine the law dealing with privacy in medical information, and
- examine models and rules to protect privacy, and determine whether new technologies can ensure privacy in the area of medical records.

To accomplish these objectives, OTA sought the opinions, attitudes, and perceptions of the stakeholders in academia, medicine, and the legal profession; researchers in computer and information system security; government agencies; and public interest groups. This was accomplished through interviews, correspondence, and public participation in two workshops.[2]

OTA explored the issue of privacy in computerized medical information by addressing questions such as:

What are the issues with respect to privacy in paper systems for health information? How will these issues change with computerization? What new issues will arise?

- To what extent can technology address the confidentiality and privacy of computerized health care information? What are the limitations of the technologies? Are the most serious threats to privacy internal to the computer systems designed for this information, external to them, or both?
- What is the impact of creating a large databank of easily accessible health care information? What kind of uses will there be for the information? Will additional demands for information be spurred by its ready availability? How must these demands for information be dealt with?
- How must underlying issues, such as the perceived need for a unique patient identifier, the content of the patient record, and patient consent to disclosure of information, be addressed?
- How has the law traditionally dealt with concerns about privacy in medical information? What role might new legislation play in addressing these concerns?

What Is Health Care Information?

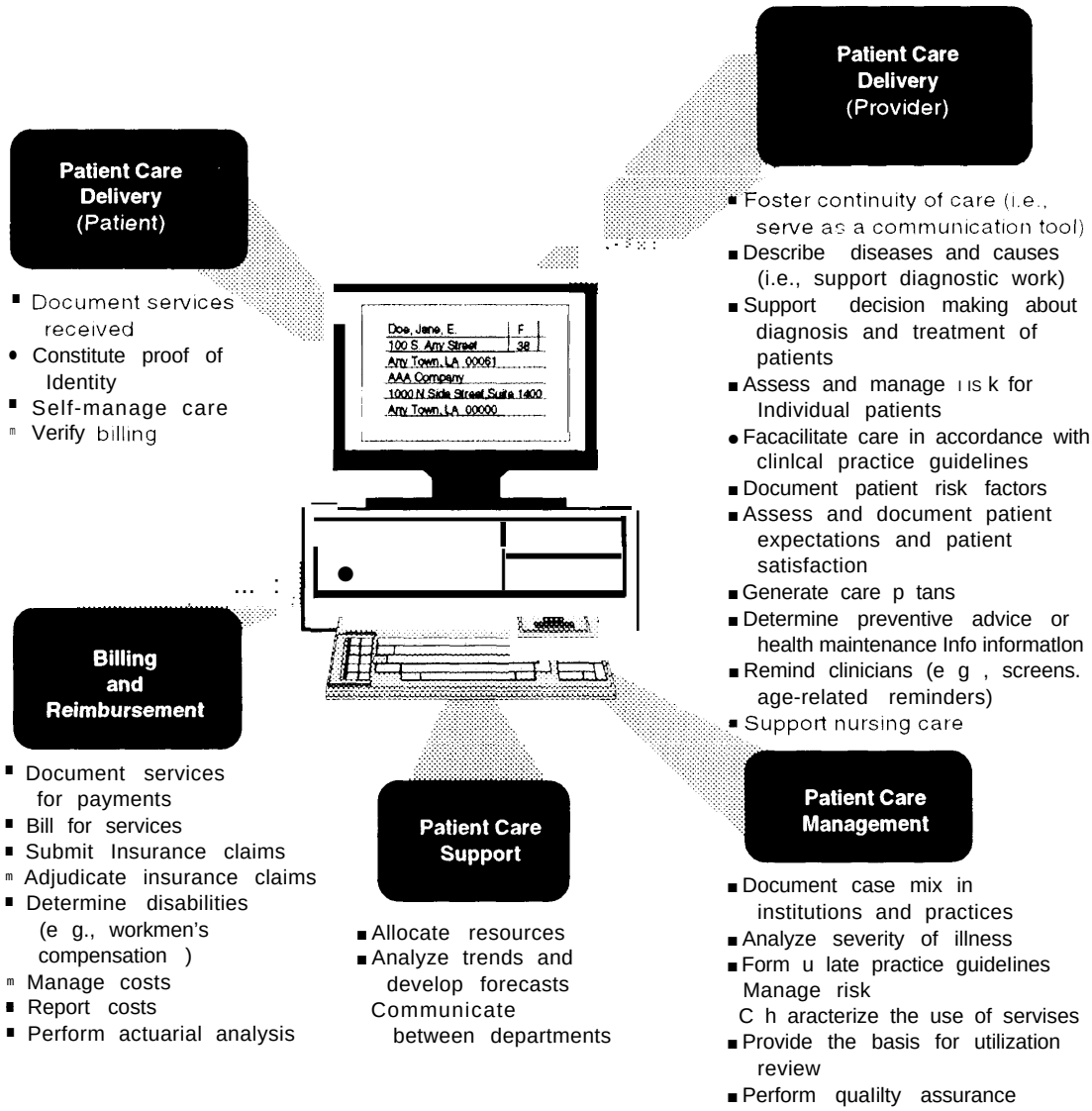
The Institute of Medicine report, *The Computer-Based Patient Record: An Essential Technology for Health Care*[3] (hereinafter referred to as the "IOM report") recommends that health care professionals and organizations should adopt the computer-based patient record for use in online systems as the standard for medical and all other records related to patient care. Computer-based patient records would replace the present system of paper records. Whether on paper or in electronic form, the information contained in patient records is the core of what is often understood to be "health care information,' information about patients generated and maintained throughout the health care industry in providing health care services (see figure l-l). But the patient record, generated and maintained by the health care provider and the patient in the course of the patient's health care, is only a part of the health information collected and maintained on individuals.[4] Parties who are not directly involved in patient care also gather and maintain health care

[2] OTA workshops, "Emerging Privacy Issues in the Computerization of Medical Information,'' July 31, 1992; and "Designing Privacy in Computerized Health Care Information,'' Dec. 7, 1992.

[3] Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care,* Richard S. Dick and Elaine B. Steen, eds., (Washington DC: National Academy Press, 1991), p. 51. This is a publication of the Committee on Improving the Patient Record, Division of Health Care Services.

[4] Joan Turek-Brezina, Chair, Department of Health & Human Services Task Force on the Privacy of Private Sector Health Records, personal communication, April 1993.

Figure I-I—Primary Uses of Patient Records

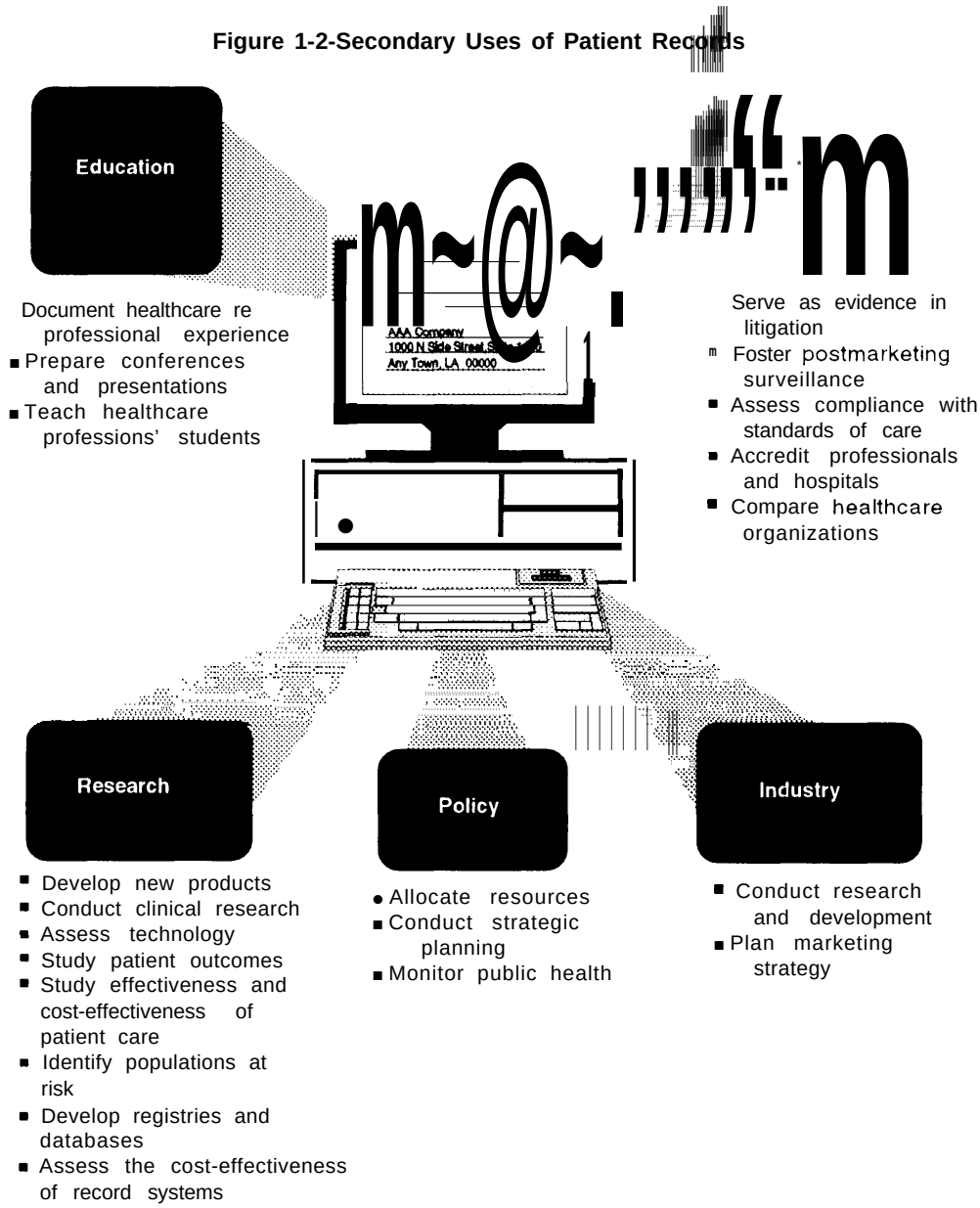


SOURCE: American Health Information Management Association (AHIMA), 1993, based on information contained in Institute of Medicine, The Computer-Based Patient *Record:An Essential Technology for Health Care,* Richard J. Dick and Elaine B, Steen, eds., (Washington, DC: National Academy Press, 1991).

information, and are often referred to as *secondary users* of the information. (For further discussion of secondary users of health care information, see box 2-F, and ch. 2). Among these are educational institutions, the civil and criminal justice systems, pharmacies, life and health insurers,[5] rehabilitation and social welfare programs, credit agencies and banking centers, public health

[5] Some commentators contend that health care claim reimbursement processing has become such a major and integral part of the delivery of health care that health care insurers are among the primary users of patient information. In figure 1-1, the American Health Information Management Association shows billing and reimbursement as a primary use of patient records.

Figure 1-2-Secondary Uses of Patient Records



SOURCE: American Health Information Management Association (AHMA), 1993, based on information contained in Institute of Medicine, *The Computer-&.sedPa tient Record:An Essential Technology* Health *Care,* Richard J. Dick and Elaine B. Steen, eds., (Washington, DC: National Academy Press, 1991).

agencies, and medical and social researchers (see figure 1-2)$_0$

As a result, in exploring appropriate ways to protect privacy, proposed definitions of what constitutes ''health information' or ''health care information vary, but tend to consider health care information to be inclusive of more than the patient record itself. The American Medical Association's (AMA's) Proposed Revisions to its Model State Bill on Confidentiality of Health

Care Information defines the term "confidential health care information" as:

> . . . information relating to a person's health care history, diagnosis, condition, treatment, or evaluation, regardless of whether such information is in the form of paper, preserved on microfilm or stored in computer-retrievable form.

The American Health Information Management Association's Health Information Model Legislation Language refers to ''health care information' even more broadly as:

> . . . any data or information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient or other record subject; and 1) relates to a patient's health care; or 2) is obtained in the course of a patient health care from a health care provider, from the patient, from a member of the patient's family or an individual with whom the patient has a close personal relationship, or from the patient's legal representative.

This report will refer to health care information as defined in this manner. This definition includes a range of medical information generated, gathered, and stored about individuals. It recognizes that the full range of health care information must be protected.

THE NEED FOR PRIVACY IN HEALTH CARE INFORMATION

Health information and the medical record include sensitive personal information that reveals some of the most intimate aspects of an individual's life. In addition to diagnostic and testing information, the medical record includes the details of a person's family history, genetic testing, history of diseases and treatments, history of drug use, sexual orientation and practices, and testing for sexually transmitted disease. Subjective remarks about a patient's demeanor, character, and mental state are sometimes a part of the record.

A medical information computer searching center.

The medical record is the primary source for much of the health care information sought by parties outside the direct health care delivery relationship, such as prescription drug use, treatment outcomes, and reason for and length of hospital stay. These data are important because health care information can influence decisions about an individual's access to credit, admission to educational institutions, and his or her ability to secure employment and obtain insurance. Inaccuracies in the information, or its improper disclosure, can deny an individual access to these basic necessities of life, and can threaten an individual's personal and financial well-being.

Yet at the same time, accurate and comprehensive health care information is critical to the quality of health care delivery, and to the physician-patient relationship. Many believe that the efficacy of the healthcare relationship depends on the patient's understanding that the information recorded by a physician will not be disclosed. Many patients might refuse to provide physicians with certain types of information needed to render appropriate care if patients do not believe that

information would remain confidential.[6] (For a discussion of the distinction between the terms "privacy" and "confidentiality" and for definitions of these terms for purposes of this report, see box l-A) In addition to serving the physician-patient relationship and the delivery of personal health care, this information is a source of important data for insurance reimbursement. When aggregated, it can assist in monitoring quality control of health care delivery by providing resources for medicalresearch. The lack of proper protections for privacy could lead to (and has, in some cases) the physician' swithholding information from a record, maintaining a second complete record outside of the computerized system, or at the extreme, creating a market for health care delivered *without* computer documentation.[7] Safe*guards to privacy in individual health care information are imperative to preserve the health care delivery relationship and the integrity of the patient record.*

Health information and the medical record include sensitive personal information that reveals some of the most intimate aspects of an individual's life.

Many interests compete in the collection, use, and dissemination of medical records. In the case of *United States of America v. Westinghouse Electric, the Court* of Appeals for the Third Circuit set guidelines to be used by a court in weighing the individual's privacy interest in medical records against the need for public agency access to information.

> Thus, as in most other areas of the law, we must engage in the delicate task of weighing competing interests. The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record is generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy or other recognizable public interest militating toward access.[8]

Similarly, whatever the technology employed to computerize medical information, decisions about data privacy also involve striking a balance, in this case between the individual's right to privacy against the cost of security, the inherent impediment security measures present to the ready accessibility of data, and the societal benefits of access to information. On the basis of the Institute of Medicine's report and the consensus among stakeholders that computerization will go forward, OTA did not analyze the question of whether computerization of patient information is appropriate to the interests of individual privacy.

THE COMPUTERIZATION OF MEDICAL RECORDS

While some aspects of the health care industry continue to rely on a paper record system, in recent years, individual medical practices and institutions have computerized parts of their recordkeeping. Computer software vendors have developed systems to streamline record-keeping and administrative functions. Traditionally, however, computer systems for patient information have been largely associated with medical centers, hospitals, or offices. Departments within

---

[6] U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington DC: U.S. Government Printing Office, 1977), p. 28.

[7] OTA Workshop, July 31, 1992, op. cit., footnote 2.

[8] 638 F.2d 570 (3rd Cir. 1980).

Box I-A–The Problem of Definition–Privacy and Confidentiality

In discussions about privacy and information policy, the terms privacy and *confidentiality* are often used interchangeably. Neither term possesses a single clear definition, and theorists argue variously that privacy and confidentiality (and the counterpart to confidentiality, secrecy) maybe concepts that are the same, completely distinct, or in some cases overlapping.

While definitions of privacy and confidentiality and distinctions between the two cannot be tightiy drawn (as indeed, the two terms are not necessarily exclusive of one another), for purposes of this report, OTA will attempt to use the terms in the following ways, largely mirroring approaches to the subject matter taken by Alan Westin and Charles Fried. Confidentility will refer to how data collected for approved purposes will be maintained and used by the organization that collected it, what further uses will be made of it, and when individuals will be required to consent to such uses. It will be achieved, as Anita Aen states, when designated information is not disseminated beyond a community of authorized knowers. According to Allen, confidentiality is distinguished from secrecy, which results from the intentional concealment or withholding of informational *Privacy will* refer to the balance struck by society between an individual's right to keep information confidential and the societal benefit derived from sharing the information, and how that balance is codified into legislation giving individuals the means to control information about themselves.

"Privacy" can be viewed as a term with referential meaning; it is typically used to refer to or denote something, But "privacy" has been used to denote many quite different things and has varied connotations. As Edward Shils observed 20 years ago:

> Numerous meanings crowd in the mind that tries to analyze privacy: the privacy of private property; privacy as a proprietary interest in name and image; privacy as the keeping of one's affairs to oneself; t he privacy of t he internal affairs of a voluntary association or of a business; privacy as the physical absence of others who are unqualified by kinship, affection or other attributes to be present; respect for privacy as the respect for the desire of another person not to disclose or to have disclosed information about what he is doing or has done; the privacy of sexual and familial affairs; the desire for privacy as the desire not to be observed by another person or persons; the privacyof the private citizen as opposed to the public official; and these are only a few.

Definitions of privacy maybe narrow or extremely broad. One of the best known definitions of privacy is that set forth by Samuel Warren and Lmuis Brandeis in a 1890 article that first enunciated the concept of privacy as a legal interest deserving an independent remedy. Privacy was described as "the right to be let alone."2 In spite of its breadth, this view has been influential for nearly a century.[3] In the 1960s, 1970s, and 1980s, the proliferation of information technology (and concurrent developments in the law of reproductive and sexual liberties) has inspired further and more sophisticated inquiry into the meaning of privacy.[4]

---

1 Anita L. Allen, *Uneasy Access: Privacy For Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988), p. 24.

2 The term "the right to be let alone" was borrowed by the authors from the 19th century legal scholar and jurist, Thomas Cooley. See T. Cooley, *Law of Torts* (2d ed. 1888).

3 Allen argues that if privacy simply meant "being let alone," any form of offensive or harmful conduct directed toward another person could be characterized as *a* violation of personal privacy.

4 Anita L. Allen, op. cit., footnote 1, p. 7.

(Continued on next page)

Box I-A–The Problem of Definition-Privacy and Confidentiality-Continued

In his work *Privacy and Freed@,* Alan Westin conceived of privacy as "an instrument for achieving individual goals of self realization," and defined it as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others," approaching the concept in terms of Informational privacy. W. A. Parent defined privacy in terms of information as "condition of not having undocumented personal information about oneself known by others."[6]

In contrast, Ruth Gavison defines privacy broadly as "limited access in the senses of solitude, secrecy and anonymity." In her view, "privacy" is a measure of the extent to which an individual is known, the extent to which an individual is the subject of attention, and the extent to which others are in physical proximity to an individual. Her definition of privacy was to include:

> . . . such "typical" invasions of privacy as the collection, storage, and computerization of information; the dissemination of information about individuals; peeping, following, watching, and photographing individuals intruding or entering "private" places; eavesdropping, wiretapping, reading of letters, drawing attention to individuals, required testing of individuals; and forced disclosure of information.[7]

In *Computers, Health Records, and Citizens Rights,* Westin draws a clear distinction between the concepts of privacy and confidentiality in the context of personal information.

> Privacy is the question of what personal information should be collected or stored at all for a given social function. it involves issues concerning the legitimacy and iegality of organizational demands for disclosure from individuals and groups, and setting of balances between the individual's control over the disclosure of personal information and the needs of society for the data on which to base decisions about individual situations and formulate public

5 Alan F. Westin, *Privacy and Freedom* (New York, NY: Atheneum, 1967).

6 W. A. Parent, "Recent Work on the Conception of Privacy," *American Philosophical Quarterly,* vol. 20,1983, p. *341.*

7 Ruth Gavison, "Privacy and the Limits of Law," M/e *LawJournal,* vol. 89, 1980, p. 421.

these facilities have been linked to provide for access and exchange of information among practitioners and administrators within an institution. Currently, however, the health care industry is moving toward linking these institutions through a proposed *information infrastructure* (computers and information system) and the communications networks.

The IOM report advocates computerization of patient records and health care information in online systems to improve the quality of patient care, advance medical science, lower health care costs, and enhance the education of health care professionals. It envisions that the computerized patient record will "provide new dimensions of record functionality through links to other databases, decision support tools and reliable transmission of detailed information across substantial distances.

Linkages would allow transfer of patient data from one care facility to another (e.g., from physician office to hospital) to coordinate services, and would allow collation of clinical records of each patient over a period of time among

9 Institute of Medicine, op. cit., footnote 3, p. 51.

10 Ibid.

policies. Confidentiality is the question of how personal data collected for approved social purposes shall be held and used by the organization that originally collected it, what other secondary or further uses may be made of it, and when consent by the individual will be required for such uses. It is to further the patient's willing disclosure of confidential information to doctors that the law of privileged communications developed. In this perspective, security of data involves an organization's ability to keep its promises of confidentiality.

Allen notes the unsettled relationship between secrecy and privacy in the privacy literature. In her view, secrecy is a form of privacy entailing the intentional concealment of facts. She claims that it does not always involve concealment of negative facts, as is asserted by other privacy scholars.[a] She points to the work of Sissela Bok, who defines secrecy as the result of intentional concealment and privacy as the result of "unwanted access."[9] Since privacy need not involve intentional concealment, privacy and secrecy are distinct concepts. Privacy and secrecy are often equated because "privacy is such a central part of what secrecy protects." Bok viewed secrecy as a device for protecting privacy.[10]

Charles Fried also discusses the relationship between privacy and secrecy. He states that at first glance, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. He argues for refinement of this notion, stating that is not true that the less that is known about us the more privacy we have. He believes, rather, that privacy is not simply an absence of information about us in the minds of others, it is the control have over information about ourselves. It is not simply control over the quantity of information abroad; it is the ability to modulate the qualit y of the knowledge as well. We may not mind that a person knows a general fact about *us,* and yet we feel ou[r privacy invaded if he knows the details.[11]

---

8 Ibid.

9 Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation*, (New York, NY: Oxford University Press, 1984), p. 10.

10 Ibid.

11 Charles Fried, "Privacy," *Yale Law Journal, vol. 77, 1968,* p. *474,* at p. *782.*

SOURCE: Office of Technology Assessment, 1993, and dted footnotes.

providers and at various health care sites.[10] This would provide a *longitudinal record,* one that forms a cradle-to-grave view of a patient's health care history.[11] The IOM report further envisions extraction of data by secondary users (policymakers and clinical researchers) from data in the computer-based patient record. The Report of the Workgroup for Electronic Data Interchange[12] similarly envisions electronically connecting the health care industry by an integrated system of electronic communication networks that would allow any entity within the health care system to exchange information and process transactions with any other entity in the industry. This capability, the workgroup asserts, could lead to a reduction of a administrative and health care delivery costs.

As a result of the linkage of computers, patient information will no longer be maintained, be accessed, or even necessarily originate with a single institution, but will instead travel among a myriad of facilities. As a result, *the limited protection to privacy of health care information now in place will be further strained. Existing*

11 Ibid., p. 45.

12 U.S. Department of Health and Human Services, Workgroup for Electronic Data Interchange, Report to the Secretary, July 1992.


JOHN STEY, UNIVERSITY OF CONNECTICUT HEALTH CENTER

A health care practitioner searches an online medical research database,

models for data protection, which place responsibility for privacy on individual institutions, will no longer be workable for new systems of computer linkage and exchange of information across high performance, interactive networks. New approaches to data protection must track the flow of the data itself.

Smart cards have been proposed as a means to computerize and maintain health care information. A smart card is a credit card-sized device containing one or more integrated circuit chips that can store, process and exchange information with a computer (see figure 1-3). Smart card systems are used on a limited basis in some areas of the United States for medical purposes. They are used on a wide scale in France, and are being tested in other European countries to facilitate delivery of health care services. Smart cards can function in two ways: 1) to store information, which can be accessed when a patient presents the card to a health care practitioner, and/or 2) as an access control device, carrying out security functions to maintain a more secure and efficient access control system for health care information computer systems.

Some describe smart cards as the ultimate in a distributed database that can meet the needs for access control and consent to disclosure, but critics cite shortcomings of the cards with respect to patient privacy. Among these is the proposal that such a system involve a backup database of information that is contained on each card, which would arguably present many of the same privacy problems that an online system would have.[13] (For a discussion of the privacy challenges presented by online systems and smart card systems, see box l-B). Some are concerned that individuals may not even know the content of the information they are carrying on the card.[14] Others worry that the card marks a step in a move toward a national identification card, and that individuals will at some point be asked to present a card for identification purposes that contains a tremendous amount of highly personal information.[15]

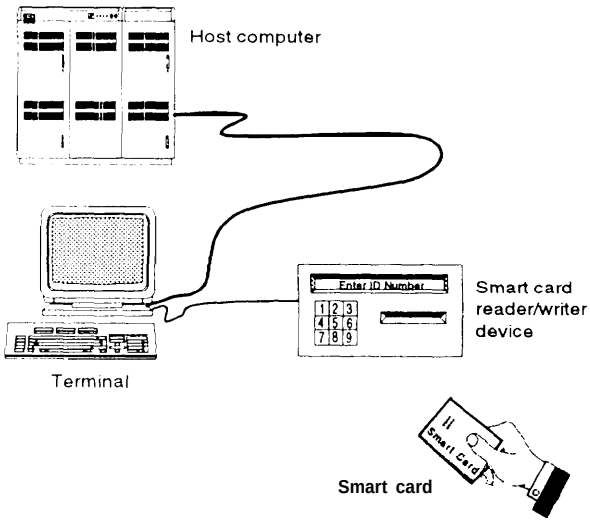
---

13 Criticism of the smart card approach stems largely from the proposal that Such a system involve a backup database of information that is already contained on the card. In and of themselves, smart cards may well offer some solutions to protecting privacy if information contained on them is properly segmented. Sheri Alpert, "Medical Records, Privacy and Health Care Reform,'' prepublication draft, June 29, 1993. A version of this paper will appear in the November/December issue of *The Hastings Center Report*. For further discussion of smart cards, see ch. 3.

14 Marc Rotenberg, Director, Washington Office, Computer Professionals for Social Responsibility, personal communication, December 1992.

15 David Flaherty, ''Privacy, Confidentiality and the Use of Canadians Health Information for Research and Statistics,'' Canadian Public Health Administration, vol. 35, No. 1, p. 80, 1992.

Figure 1-3-Generalized Smart Card System



SOURCE: Martha E. Haykin and Robert B.J. Warnar, U.S. Department of Commerce, National Institute of Standards and Technology, "Smart Card Technology: New Methods for Computer Access Control," special publication 500-157, September 19SS.

Computerization of Health Care Information by Private Companies

In addition to efforts by the health care industry to establish an online computer network of patient records, private companies have begun to act on the commercial incentive to collect health care data. Information is, in some cases, gathered on specific individuals to assist the insurance underwriting industry; in other cases, companies offer such computer services as health insurance claims-processing, office management, or patient billing. (See box 2-F.) These companies use the medical information made available to them by gathering and selling aggregate information, usually without patient knowledge or consent (although with the knowledge of a participating physician). These practices, for the most part, are currently legal, although the businesses in question operate under no regulatory guidelines regarding security measures, use of patient identifiers, requirements for training of personnel about privacy concerns, company confidentiality policies, or protocols for gathering, selling, or transferring data. Aware of public concerns about privacy, these companies have taken steps to address the issue of confidentiality in the data through security and contfidentiality measures, employee education, and personnel and cofidentiality policies.

Security and Confidentiality Measures

For online computer systems, security is generally provided by use of user identification names and passwords, and by user-specific menus to control access to functions and to limit access of the user to the information he or she legitimately needs. In addition to these measures, some systems use audit trails to record significant events on a system that may be inspected and traced to when a suspicious event occurs. Supplementing these technological measures, organizational education, policies, and disciplinary actions attempt to ensure that confidentiality is maintained within **the** system. Smart cards can also play a role in system security, functioning as an access control device, serving the security functions that are normally carried out by the user, including entering passwords and PINs (personal identification numbers). A more extensive discussion of the use of smart cards for access control is in chapter 3, and a further discussion of computer security measures is in appendix A.

Private companies have begun to act on the commercial incentive to collect health care data.

A major focus of security and confidentiality measures is preventing privacy invasion by trusted insiders. Prosecutions of U.S. Federal Government employees for unlawful disclosure of personal information indicate the risk of invasion of privacy perpetrated by trusted insiders, who, motivated by financial incentives to supplement

Box I-B—Proposals for Medical Information Technology and Challenges to Privacy

Proposals for computer systems for collection and handling of medical information generally include online *networked systems,* as proposed by the report of the Institute of Medicine and the Workgroup for Electronic Data Interchange, and smart card system, reportedly to be proposed in the report of the Administration Task Force on Healt h Care Reform. while both approaches solve a variet y of healt h care delivery, administration, reimbursement and, in some cases, privacy problems, they also present new privacy concerns.

Online Systems

The report of the Institute of Medicine, The *Computer-Based* Patient *Record:A New Technology forHealthcare* (hereafter referred to as "the IOM study"), and the report of the Workgroupfor Electronic Data Interchange (hereafter referred to as the "WEDI Report") look toward integrated systems of electronic communication networks that would allow exchange, storage, and processing of health care information. Online networked systems would allow entities within the health care system to exchange information and process transactions with other entities in the industry, facilitate integration of patient information overtime and from one care provider to another, improve data and data access available to researchers and make research findings available to practitioners over medical information computer systems.

While acknowledging the benefits online systems provide, organizations involved in evaluating plans for computerization recognize the serious implications for privacy that are raised by use of computer databases linked electronically for information exchange. The WEDI report states that electronic technology threatens individual privacy, and that the ability to transmit data from one computer to another also enables violations of data integrity and security. The IOM study points out the concern about access from outside of computer systems by hackers. The report of the Work Group on Computerization of Patient Records notes the tremendous capacity to link data that computers provide, and that the same ability to link patient data by insurers and providers for legitimate purposes would also create opportunities for abuse. Concerns about data integrity reflect the possibility computers create for "invisible" modification, deletion or addition of data.

Smart Cards

A smart card is a credit card-sized device containing one or more integrated circuit chips, which perform the functions of a microprocessor, memory and an input/output interface. Proposals for use of

their income, sell personal information. While resources can be directed toward minimizing risk of abuse of information by insiders, *no system can be made totally secure through technology, and* ***the*** *greatest perceived threat to privacy in medical information exists in the potential for abuse of authorized internal access to information by persons within the system, whether paper or computer based.*

PROTECTION FOR PRIVACY IN HEALTH CARE INFORMATION

Privacy in health care information has been protected through primarily two sources: 1) in the historical ethical obligations of the health care provider to maintain the confidentiality of medi*cal* information; and 2) in a legal right to privacy, both generally and specifically, in health care information. *The present system of protection, for*

smart cards have been of three major kinds: Cards could be used as a means of access control; they could serve as a medium for storing and carrying the entire patient record; or they could combine the two function by providing an access control mechanism while storing certain limited patient information. Proponents of smart cards argue that they provide the ultimate distributed system, so that individual patients can maintain their own medical records, and would be empowered with the ability to consent to any access to the data by authorization of access to the card. Real-time access to information would be available only with the consent of the patient with the exception possibly of emergency information. This system contrasts with the risk of computer network penetration whereby access could be gained to thousands of clinical records.

The system presents drawbacks however, which may limit its ability to protect patient privacy. Current proposals for use of the cards for health care data suggest that the medical data reside solely on the card, but the card is useless if lost, damaged or forgotten. The proposed solution to the problem is the creation of a back-up database containing the patient information, Such a database would also address the concerns of medical researchers and accreditation organizations, whose need for aggregate data would not be well served by storage of medical records on individually held cards. Addressing these needs might require that the card serve as the patient's personal copy of his or her record, or would function as an access control tool, but would not be the sole source of patient information.

A back-up database would present many of the same problems an online computerized system would. Questions about who (insurers, researchers, public health agencies, financial institutions) would appropriately have access to information would remain, as well as concerns about abuse of the information by persons with proper access to the system. Computer banking of information with some unique identifier would occur, creating questions about linking of information, as well as the nature of the identifier.

In addition to these concerns, privacy advocates have voiced issues specific to smart cards themselves. Some have noted that, while the smart card allows for control over the information while it is in the patient's's possession, it is entirely possible that the patient will not know the nature of the information he or she is carrying on their person, so that concerns about patient access to information and informed consent would remain. They indicate uneasiness with a system of identification cards containing large amounts of personal information to be carried by individuals, and the implications such a system may have for a large-scale national identification card system.

SOURCE: Office of Technology Assessment, 1993.

health care information offers a patchwork of codes; State laws of varying scope; and Federal laws applicable to only limited kinds of information, or information maintained specically by the Federal Government. The present legal scheme does not provide consistent, comprehen - sive protection for privacy in health care information, whether it exists in a paper or computerized environment.

Ethical Sources

The physician[16] confidentiality obligation can be found in the Oath of Hippocrates, written between the Sixth Century B.C.E. and the First

[16] The Oath of Hippocrates applies to physicians. Psychologists, nurses, and others referred to as ' 'health cafe providers'' operate under different, perhaps less comprehensive, strictures. Steven Brooks, Manager, Medical Information Management, Aetna Health Plans, personal communication, April 1993,

Century B.C.E. The Hippocratic Oath provided that what the physician saw or heard in the course of treatment "which should not be published abroad' would be kept in confidence. Later codes of medical ethics included language addressing the issue of confidentiality of information. The American Medical Association's Code of Ethics has evolved since its adoption; the obligation to preserve patient confidentiality remained in the 1980 code, but without guidelines about how to respond to requests for information from secondary users of medical information, such as researchers, police, and Federal agencies. Recent AMA policy statements set forth in more detail the responsibilities of physicians with regard to confidentiality of patient information and issues surrounding the medical record. In its Code of Medical Ethics, Current Opinion, 1992, the AMA states its belief that the information disclosed to a physician during the course of the relationship between the doctor and patient is confidential to the greatest possible degree, and outlines particular instances when the obligation to safeguard patient confidences is subject to exceptions for legal and ethical reasons. Professional ethical codes do not possess the force of law, but may be enforced through bodies such as the disciplinary board of the professional organization, or may serve as evidence of a provider's breach of his or her legal duty to maintain confidentiality,

Legal Origins

Although the Bill of Rights does not specifically set forth a right to privacy, a right to privacy in information has been upheld by the Supreme Court in a series of cases beginning in the 1950s. The Court looked to the first amendment and due process clause, the fourth amendment protection against unreasonable searches and seizures and the fifth amendment protection against self incrimination as sources of the right. A later case, *Griswold v. Connecticut*[17], talked of the zone of privacy created by the first, third, fourth, fifth and ninth amendments. However, in two cases decided in 1976, the court did not recognize a constitutional right to privacy that protected erroneous information in a flyer listing active shoplifters, or one that protected the individual's interest with respect to bank records. (For futher discussion of the Supreme Court's analysis of a right to privacy, see box 2-B).

FEDERAL LAW

While some Federal laws address the question of privacy in certain information collected and maintained by the Federal Government, *no Federal statute defines an individual's specific right to privacy in his or her personal health care information held in the private sector and by State or local governments.* At the Federal Government level, the Privacy Act of 1974[18] specifically endorses the finding that privacy is a fundamental constitutional right. Designed to protect individuals from Federal Government disclosure of confidential information, the Privacy Act prohibits Federal agencies (including Federal hospitals) from disclosing information contained in a system of records to any person or agency without the written consent of the individual to whom the information pertains, and stipulates that Federal agencies meet certain requirements for the handling of confidential information.

In addition to the requirements of the Privacy Act, Federal law, by statute and implementing regulations, prescribes confidentiality requirements for records of patients who seek drug or alcohol treatment at federally funded facilities. As these regulations have the full force and effect of Federal law, they supersede State laws on confidentiality in the area of drug or alcohol treatment. Provisions of the Social Security Act also prohibit disclosure of information obtained by officers or employees of the Department of

17 381 U.S. 479, 85 S. Ct. 1678 (1965).

18 The Federal Privacy Act of 1974, 5 U.S.C. Sec. 552a **(1988).**

Health and Human Services, except as prescribed by regulation.

STATE LAWS AND REGULATIONS

At common law, States have recognized an action for invasion of privacy in the tort law. Individuals may bring an action for defamation when medical records containing inaccurate information are disclosed to an unauthorized person, when that information would tend to affect a person's reputation in the community adversely. Courts have also demonstrated a willingness to apply the ethical standards of the medical profession to compel physicians to maintain the confidentiality of information they obtain in the course of treating their patients, by enforcing those standards as part of the contractual relationship between physicians and their patients.

There is significant variation in the nature and quality of State laws regarding privacy in health care information. Among the States that have regulations, statutes, or case law recognizing medical records as confidential and limiting access to them, these are not consistent in recognizing computerized medical records as legitimate documents under the law, and generally do not address the questions raised by such computerization. The range of medical privacy laws does not address the practice of compiling medical information about patients (with or without their consent or the identification of personal information) for sale to businesses with a financial interest in the data.

This patchwork of State and Federal laws addressing the question of privacy in personal medical data is inadequate to guide the health care industry with respect to obligations to protect the privacy of medical information in a computerized environment. It fails to confront the reality that, in a computerized system, information will regularly cross State lines, and will therefore be subject to inconsistent legal standards with respect to privacy. The law allows development of private sector businesses dealing in computer databases and data exchanges of patient information without regulation, statutory guidance, or recourse for persons who believe they have been wronged by abuse of data. These laws do not address the questions presented by new demands for data prompted by computerization, and the obligations of secondary users in accessing and maintaining data. Lack of legislation in this area will leave the health care industry with an uneven sense of their responsibilities for maintaining privacy.

1 The Effect of Computers on the Question of Privacy

All health care information systems, whether paper or computer, present confidentiality and privacy problems. Among these problems are administrative errors that release, misclassify, or lose information; compromised accuracy of information; misuse of data by legitimate users; malicious use of medical information; unauthorized break-ins to medical information systems; and uncontrolled access to patient data. *Computerization can reduce some concerns about privacy in patient data and worsen others; but it also raises newproblems. While* computers offer security measures that are not available to paper systems, computerization also presents concerns about privacy and confidentiality that fall into the following categories:

> *Great variation in the nature and quality of State laws regarding privacy in health care information.*

- Computerization enables the storage of a very large amount of data in a small physical space, so that an intruder can systematically obtain large amounts of data (more than could likely be stolen on paper records) once access to the electronic records is gained.
- Networking of computer information systems makes information accessible anywhere at any

time to anyone who has access. Computers and computer networks enable a large number of people to handle or have access to information and allow for surreptitious modification, deletion, copying, or addition of data.
- New databases can be created, maintained, and expanded with ease, and computers make it possible to link data sets in ways that produce new information that was not originally intended.[19]
- The computer's ability to transmit large volumes of data instantaneously make the potential dissemination of medical information "on limitless, so that the distribution of private information will be easy and inexpensive.

The increased quantity and availability of data and the enhanced ability that computerization provides to link these data raise privacy concerns about new demands for information for purposes beyond providing health care, paying for it, or assuring its proper delivery. Among these concerns is that information more easily gathered, exchanged, and transmitted will be sought and acquired by more parties for uses not connected to health care delivery-parties that may have little concern about the confidentiality of the data in their possession and individual privacy.

SPECIAL POLICY PROBLEMS RAISED BY COMPUTERIZATION

A computer-based patient record of the type recommended by the Institute of Medicine study—in which the record is linked among records or record systems of different provider institutions and to other databases and sources of information, including medical practice guidelines, insurance claims, and disease registries/and databases that contain scientific literature, bibliographic and administrative information-requires resolution of policy issues, such as the use of a *unique patient identifier, informed patient consent* to information disclosure, *standardization,* and *new demands for access* by secondary users. It *is important to resolve these issues at the outset of the computerization process, so that system designers can build into software the appropriate mechanisms to implement privacy policy.*

1 The Unique Patient Identifier

Proponents of computerized medical information recommend the use of a *unique patient identifiet* to be assigned to a patient at birth and remain permanently throughout the patient lifetime. A unique patient identifier, it is believed, would assure appropriate, accurate information exchange among approved parties, prevent fraud and forgery in reimbursement, and ensure accurate linkage of information. While a variety of approaches to establishing such an identifier have been proposed, the one most often mentioned is the use of the Social Security number as the most efficient and cost-effective way of identifying patients. Privacy advocates strongly object to this proposal. They cite the increasing use of the number in the private sector, and the power' of the number to act as a key to a variety of information in both the public and private sector and to facilitate linkage of information.[21] Proponents Of its use believe that, with appropriate precautions, the integrity of the Social Security number can be maintained. Although there is a belief that the Social Security number is now a de facto national identifier (even though this is prohibited by law), use of the number as a unique patient identifier still requires close examination. *The use of the Social Security number as a unique patient identifier has far-reaching ramifications for individual health care information privacy that*

19 Ontario Commission of Inquiry into the Confidentiality of Health Information, Report of the Commission Ontario, Canada, September 1980, vol. *2, pp. 160-166.*

20 Institute of Medicine, op. cit., footnote 3, p. 44.

21 william M. Bulkeley, ''Get Ready for Smart Cards in Health Care," *The Wall Street Journal, May 3, 1993,* p. B11.

should be carefully considered before it is used for that purpose.

Informed Patient Consent to Information Disclosure

Because computerization of medical information creates the potential for increased demands for data for purposes beyond providing health care, paying for it, or assuring its proper delivery, computerized medical information challenges present practices for providing informed consent to disclosure.

Informed consent to disclosure of information generally involves four main elements:

1. information about what data is to be disclosed must be given to the patient,
2. the patient must understand what is being disclosed,
3. the patient must be competent to provide consent, and
4. the patient's consent must be voluntary.

The present approach to providing "informed consent" challenges the concept with respect to disclosure to the patient, patient competence, and patient comprehension about what is being disclosed. In spite of the requests made of them to authorize disclosure of medical information for medical and nonmedical purposes, patients traditionally have difficulty gainin g access to inspect their own medical records, and laws governing patient access to records are neither universal nor uniform.

It is argued by some that without knowledge of what is contained in the record, patients' consent to disclosure cannot be said to be informed per se. In taking responsibility for the care of a patient, physicians have been granted broad discretion to withhold information from the patient that he or she deems to be potentially harmful.

Recent articles indicate a change in thinking about this approach, and the position of the American Health Information Management Association (AHIMA) reflects the balance of opinion as reflected by the literature. AHIMA's position is that the computerized health care record, and its potential for increased use both within and beyond the health care relationship, requires that patients have greater access to their medical record, coupled with a general atmosphere of increased patient education and involvement in his or her own health care. *Resolution of* the *question of patient access to one's record so that consent to disclosure is, in fact, informed, is critical to confronting privacy concerns about the computerized health record.*

The element of voluntariness is also challenged by the present scheme of providing informed consent. Medical information is usually required to provide health care reimbursers with sufficient information to process claims. Since individuals are, for the most part, not able to forego health care reimbursement benefits, they really cannot make a meaningful choice whether or not to consent to disclosure of their health care information. Some commentators suggest that alternative schemes to deal with the need to disclose patient information might be adopted.

1 Standards

Industry organizations are developing standards for patient-record content, data exchange formats, vocabulary, patient-data confidentiality, and data systems security. Standardization of medical information in both content and format is believed to be important to the computerization effort. Content uniformity would assure data completeness for medical practitioners. In addition, third-party payers could process claims readily on the basis of the medical, financial, and administrative information at their disposal; and secondary users of the information, such as researchers, utilization review committees, and public health workers, could anticipate the nature of the information available to them. Format standards would assure uniform and predictable electronic transmission of data.

Standards for patient-data confidentiality and data systems security would ensure that patient data are protected from unauthorized or inadvertent disclosure, modification, or destruction. Primary and secondary users of health care data are working to agree on common levels of data protection so they can benefit from use of automated patient information.

1 Outbound Linkages to Secondary Users and the Problem of Increased Demand

The Institute of Medicine report foresees broad connectivity in a computerized records system, meaning that the record or record system will establish links or interact effectively with providers' systems and databases. In addition to linkages that will connect clinical records of a single patient to create a longitudinal patient record, the report foresees external linkages to other databases and other sources of information. *These* linkages might include databases that contain scientific literature and bibliographic information, administrative information, medical practice guidelines, insurance claims, and disease registries. The IOM report acknowledges that outbound linkages create additional concerns about maintaining privacy and require tight security measures.

The power of computers to allow gathering, storage, exchange, and transmission of data could prompt increased demands for use of medical information beyond the traditional uses.

In addition to the question of security and privacy in the linked information, the larger question arises as to the appropriateness of access to information by certain parties. Policy decisions at the Federal and State levels have, over time, made medical records and health care information, as it exists in paper record form, available to utilization review agencies, medical researchers, judicial proceedings, public health agencies, licensing agencies and, in some cases, employers. *The power of computers to allow gathering, storage, exchange, and transmission of data could prompt increased demands for use of medical information beyond the traditional uses.*

MODELS FOR PROTECTION OF COMPUTERIZED MEDICAL INFORMATION

Health professional organizations, privacy advocates, and academics specializing in health information privacy have proposed legislative schemes and practice guidelines to protect privacy in medical information. These initiatives are generally based on fundamental principles of *fair information practices. These* principles, which have been implemented in the Privacy Act for the protection of federally maintained information, are as follows:

1. No personal data recordkeeping system may be maintained in secret.
2. Individuals must have a means of determining what information about them is in a record and how it is used.
3. Individuals must have a means of preventing information about them obtained for one purpose from being used or made available for other purposes without their consent.
4. Individuals must have a means to correct or amend a record of identifiable information about themselves.
5. Organizations creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuses of the data.

Health care information protection schemes usually provide individuals with certain rights:

1. The proposals address concerns about privacy in personal medical information on individuals.

2, Individuals are given the right to access much of the personal information kept on them.
3. Limits are placed on the disclosure of certain personal information to third parties.
4, Health care personnel are required to request information directly from the individual to whom it pertains, whenever possible.
5. When health care personnel request personal information from an individual, the individual must be given notice as to the authority for the collection of data, whether the disclosure is mandatory or voluntary.
6. The individual may contest the accuracy, completeness, and timeliness of his or her personal information and request an amendment.
7. The health care personnel must decide whether to amend the information within a fixed time, usually 30 days after receiving a request.
8. The individual whose request for change is denied may file a statement of disagreement, which must be included in the record and disclosed along with it thereafter.
9. The individual is given a means of seeking review of a denied request.

Chapter 4 discusses the provisions of the Massachusetts State Code on Insurance Information and Privacy Protection, Ethical Tenets for Protection of Confidential Clinical Data, the Uniform Health Care Information Act (implemented in Montana and Washington), and Model Legislation Language of the American Health Information Management Association, and their applicability to new health care information privacy legislation. While these principles form the foundation for information privacy protection, any new legislation must also reflect the development of distributed processing, sophisticated database management systems, and computer networks; and the wholesale use of microcomputers that characterize the kind of system envisioned for health care information. New legislation must also take into account access to records and security of information flows.

Current legislation at the State and Federal level for protection of privacy in medical information is limited in its application to individual institutions; the ease with which information will be transmitted between institutions requires that the law track the information, wherever it may reside, Technology may facilitate the policy goals of such a protection system. A system of audit trails and user identification codes can assist in the identification of points of unauthorized access.

CONGRESSIONAL OPTIONS

As computerization of patient records goes forward, Federal legislation is necessary to address issues of patient confidentiality and privacy .22 The present system of protection is a patchwork of State laws, which do not take into account a computerized system in which information will be frequently and easily transferred across State borders.

Option la. Congress may wish to allow computerization to go forward under the present State and Federal systems of protection.

No computer system can be made entirely secure. Privacy in health care information, whether electronic or paper, is protected by a range of various Federa1[23] and State laws. These laws are often inadequate, and in some States do not exist. The introduction of computerized medical records entails transfer of that information among participants in the health care delivery system

22 OTA Workshop, Dec. 7, 1993, op. cit., footnote 2.

23 Federal law protects privac, in only those medical records maintained by the Federal Government, e.g., records maintained on Medicare and Medicaid patients. Those Federal laws do **not** protect the records of the same patients maintained by their private physician or held by their hospital,

located in different States and operating under different State laws.

If not modified, the present patch work of laws regarding patient health care information will likely require that resolution of issues of individual privacy and improper use of medical information be left to State legislatures and State courts. They would also require that the health care industry educate itself, on a State-by-State basis, about its obligations to secure and keep confidential medical records. After a period of allowing the system to work in this way, Congress may find itself re-evaluating the question of State versus Federal legislation.

Option lb. Enact a comprehensive health care information privacy law.

As the **greatest** concerns about privacy lie in the potential for abuse of information by authorized parties with appropriate access to a computer system, legislation providing criminal and civil ecourse for illegally obtaining or disclosing records containing individually identifiable information to persons not entitled to receive it could address the problem of information brokering and illegal trafficking of health care information. The law would provide appropriate sanctions to deter such activities.

Such legislation would:

1. Define the subject matter of the legislation, ‘‘health care information,’ broadly, including the range of information generated, collected and maintained about individual patients;
2. Provide criminal and civil sanctions for improper possession, brokering, disclosure, or sale of health care information with penalties sufficient to deter perpetrators;
3. Establish rules for patient education about information practices as applied to health care information, including access to information, amendment, correction and deletion of information, and creation of databases;
4. Establish requirements for informed consent by patients to disclosure of health care information;
5. Structure the law to track the flow of health care information, incorporating the ability of computer security systems to alert supervisors to leaks and improper access to information so that the law can be applied to the information at the point of abuse, not simply to one “home’ institution; and
6. Establish protocols for access to health care information by secondary users, and determine their rights and responsibilities in the information they access.

As part of this legislative effort, Congress may want to *commission an investigation of abuses of medical information* to pinpoint the nature and scope of abuses in this area, and to provide empirical evidence of the problem in the United States.

Option 2, Monitor standard setting

Congress may wish to monitor and/or participate in efforts to set standards for the content of the medical record and the minimum level of security and confidentiality in computerized medical record systems, to assure that technological standards will facilitate privacy policy goals. This task could be delegated to a special task force made up of technology, privacy, and health information experts. Or it could be delegated to a committee charged with ongoing review of medical information privacy issues.

Option 3. Establish a special committee or commission to oversee the protection of health care data; to provide ongoing review of privacy issues arising in the area of health care information; to keep abreast of developments in technology, security measures, and information flow; and to advise the Congress about privacy matters in the area of health care information.

Computer systems for medical information and the security measures available for those systems

are in constant development, and legislation is challenged by a technology that changes quickly. Demands for data change with ' 'need" and tend to increase over time; simply relying on each individual's efforts to monitor and protect his or her privacy are useless because, in most cases, they can act only after damage has occurred. A committee or commission to oversee data protection in medical data could be modeled on proposals for a broader Data Protection Board,[24] but with a focus on health care information. A committee or commission could monitor and evaluate implementation of statutes and regulations enacted to protect privacy in health care information; it could continue research into areas of concern about privacy in health care information to supplement mechanisms by which citizens could question propriety of information collected and used by the health care industry. In this way, it would provide a measure of protection *prior* to the establishment and development of new databases and new uses for medical data. Such an entity would add a layer of protection to a legislative scheme by serving as a watchdog for potential encroachment on individual privacy in medical information, and serve as an early warning system to ensure that the legislative process is dynamic enough to deal with emerging problems .25

One function of such a committee or commission might be to formulate guidelines for parties involved in computerization of medical information, whether for purposes of health care delivery or for commercial use of data, including an outline of the responsibilities of secondary users of information in maintaining security and confidentiality of the data.

Computer security measures can only provide a certain level of protection for data in a computer system, Technology *alone* cannot completely secure a system, but appropriate operation standards and data security policies can further improve the protection of data. A regulatory scheme mandating such measures could establish a threshold of protection for computerized medical data. Such a scheme could include procedures for informing the patient about record keeping practices, disclosure of patient information, release of data to secondary users, examination, correction and amendment of the patient record by the patient, as well as provisions for internal and external review. Secondary users of information, such as medical researchers and public health agencies would be required to meet certain criteria in handling information it receives. Criminal sanctions could exist for failing to comply with regulations for maintenance of the system according to regulations.

Various efforts have been made in the private sector to gather and aggregate medical data. As such compilation of data is largely invisible and done without the knowledge or permission of the patient, a committee or commission could examine the propriety of the activity in terms of individual privacy. If the activity is considered appropriate, a regulatory scheme would be necessary to protect individual privacy.

---

24 Hearing before the Subcommittee on Social Security and Family Policy of the Committee on Finance, U. S. Senate, on Privacy of Social Security Records, Feb. 28, 1993, U.S. Government Printing Office, Washington DC: 1992, testimony of Marc Rotenberg, Director, Washington Office, Computer Professionals for Social Responsibility. See also, David H. Flaherty, ' 'Ensuring Privacy and Data Protection in Health and Medical Care, " prepublication draft, Apr. 5, 1993, Such a board has been established in several foreign counties, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Ireland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia, For an analysis of data protection in certain of these countries, see David A. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill, NC: The University of North Carolina Press, 1989).

25 Discussion of a larger scale Data Protection Board reviewing data privacy issues generally is beyond the scope of this inquiry. However, literature discussing proposals for a Data Protection Board is illustrative of the nature and function of oversight bodies for privacy in personal data.