Patient Care Management Systems, Medical Records, and Privacy: a Balancing Act

MARC D. HILLER, DrPH
LEE F. SEIDEL, PhD

WITH THE GROWTH of our information-oriented society and the increasing demands for financing and quality assurance, the collection, analysis, and storage of data related to medical care have become more complex. Over the past 50 years medical recordkeeping has evolved to keep pace with the changes and growth of the health care system, and many significant advances have resulted from the adaptation of modern computer technology to the health industry.

Recent advances in computer technology have permitted the accumulation, analysis, and storage of an unlimited quantity of medical records and medical record information, thereby seriously compounding existing controversies surrounding patient confidentiality and privacy (*1*). (For this paper, we define a medical record as a record, file, document, or other written material relating to a person's medical history, diagnosis, condition, treatment, or evaluation that is created by a health care provider. Medical record information or medical record data constitute information obtained from a medical record or from a patient, his or her spouse, or legal guardian for the purpose of making a nonmedical decision about that patient.)

Patient care management systems (PCMS) constitute a combination and expansion of computerized medical record systems used for clinical care services (such as PROMIS, based on the problem-oriented record system devised by Lawrence L. Weed at the University of Vermont Medical Center) and basic management information systems used largely for financial purposes (such as those created for business and industry). The continuing evolution and refinement of these systems mark the linkage between the delivery of clinical patient care services and the management and financing of organizations providing such services. This junction is expanding, based on the need confronted by hospitals to render detailed bills for patient services. This need has stimulated the formation of fully integrated PCMS that can capture, store, and report every significant episode of treatment for a specific patient and its associated cost. Whereas ethical standards concerning the release and use of patient care information traditionally have been a linchpin of the medical records profession, computerization of medical records and the integration of medical and financial data have diluted this traditional safeguard.

A 1975 survey of some 6,000 hospitals by the American Hospital Association (AHA) revealed that about 1,500 had inhouse computers; this number surely has multiplied since then with the advent of minicomputers and increased experimentation with information systems (*2*). Thus, it seems that PCMS undoubtedly will become almost inevitable in health care institutions.

From the standpoint of health care administration, PCMS inevitably will continue to gain importance with further strivings toward efficiency, control, and cost effectiveness in management and decision making. Al-

The authors are in the Health Administration and Planning Program, School of Health Studies, University of New Hampshire, Hewitt Hall, Durham, N. H. 03824. Tearsheet requests to Dr. Marc D. Hiller.

most a decade ago, Bekey (*3*) of the University of Southern California proclaimed that "It is evident that hospital information systems have moved from being a luxury to being a necessity in the growing progressive modern hospital." In the 1980s, advances in health services management are likely to overshadow the clinical applications of such systems.

Current trends suggest that the application of computer technology to health care management will be essential in an era of cost containment, fiscal restraint and responsibility, and government intervention through planning, financing, and regulation. For many of the same reasons that automation is attractive to other sectors of society, computerization and the development of PCMS are increasingly gaining popularity in the health care industry. This expansion in use is attributable to increasing demands and expectations for medical care services, heavy increases in the volume of paperwork, the need for rapid transmission of data, increases in annual hospital admissions and ambulatory care services, and increased mandatory reporting to Federal and State governments. When used properly, PCMS can disseminate information to the appropriate people at the proper time and thus benefit the patient individually and society collectively.

From an institutional care perspective, few large hospitals or medical centers can operate successfully and cost effectively in the 1980s without complex and intricate computer data systems. Furthermore, hospitals must increasingly address this technology and apply it as a means of addressing specific health care problems (*4*). Some institutions, such as the Maine Medical Center in Portland and the El Camino Hospital in Mountain View, Calif., already have expanded their systems to maintain patients' charts with daily entries made directly into the computer by physicians, nurses, laboratory personnel, and other health care personnel. At Beth Israel Hospital in Boston, research is underway to facilitate direct entry of the patient's medical history information into its system. For physicians, breakthroughs in the use of PCMS in diagnoses and clinical decision making are expected soon as a result of continuing research in major medical centers.

Additional positive outgrowths of using such systems in medical treatment and research include better therapies, more prompt diagnosis and treatment of illness, the matching of appropriate organ transplant donors and recipients, the determination of drug interactions and protocols, the study of genetic diseases, and the discovery of lifesaving technologies, to cite only a few. Somewhat removed from the actual use of PCMS in the administration and delivery of medical care is the increased demand for and subsequent use of medical record data in utilization and standards reviews, epidemiologic studies, program evaluations, and biomedical, behavioral, and health services research. Thus, the societal trend toward dependence on computers for the collection, maintenance, storage, management, and analysis of patient care data appears to present significant opportunities and positive advances in the health care industry.

However, the computer can also pose major threats to privacy and increase depersonalization and dehumanization in the practice of medicine, the management of health facilities, and the conduct of research. This expanded use of computers—albeit on two separate, parallel tracks, that is, for medical record purposes and for institutional management—has introduced new and complex social and ethical dilemmas into institution-based care. According to Westin (*5a*):

> As American society redefines and reorganizes its health care system in the coming decade, it will have to make increased use of computer technology to manage the rivers of data that will be generated . . . If the question is not whether but how such technology will be used in health care, American Society has one non-negotiable condition for this process: basic citizen rights cannot be made a casualty of technology-assisted health systems. To do so would be to betray the tradition of Hippocrates, and ultimately to dehumanize health care itself.

Universal concern (*5,6–12*) has been expressed about which data are being tabulated and used, the extent of their accuracy, the need to control their dissemination, and the extent to which patients may have access and opportunity to verify and correct their personal records. Although the issues of privacy and confidentiality did not arise with the invention of computers (*13*), interest has heightened with the proliferation of data handled by them because of their expanding technological capabilities (*14,15*). Furthermore, necessary access to medical records for management purposes is being given more and more to nonhealth professionals who have been neither sensitized to patients' concerns about confidentiality and privacy nor bound by strong ethical or professional codes of conduct regarding the usage of such information.

Recent trends toward greater reliance on computers in health data and record systems have generated increased attention to issues of confidentiality and privacy for which the establishment of sound governing institutional policies has not occurred (*16,17*). Although the Constitution, Federal and State statutes, and judicial interpretations have been instrumental in guarding patients' rights to privacy, significant efforts must still emerge from within hospitals and other health care institutions to ensure adequate safeguards. In essence, directors of such institutions should view the promulgation of standards to ensure necessary protections as institutional responsibilities rather than simply patient rights that require legal enforcement. Policies must be designed to balance personal privacy and confidentiality while not offsetting the need to make vital information quickly and easily available to physicians who require it legitimately and to other users who may have justifiable claims to it.

The flow of medical record information between hospitals and third parties is already heavily automated and likely to become more so. Moreover, the creation of large automated information systems, such as PCMS, poses new problems and opportunities from a privacy protection perspective. The problems center around the need to specify the rules under which hospital personnel shall have access to all or part of an automated medical record and the necessary levels of security for records that contain sensitive, personal information (for example, psychiatric records, abortion records, venereal disease treatment records). The opportunities arise from the fact that a computerized record can be adapted to a need-to-know policy more easily than a traditional, manual one.

Clearly, yesteryear's traditional single-sentence confidentiality oath can no longer provide the sole source on which the system of today and tomorrow can rely. Physicians, hospitals, and others need more guidance, and patients must be given additional protection (*18*). As the Privacy Protection Study Commission reported (*19a*):

> The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable. Dramatic developments in computer and communications technology, which both facilitate record-keeping functions previously performed manually and provide the impetus and means to devise new ones, can only exacerbate this problem.

Never before has a society possessed such a wealth of health and medical knowledge, equipment, and technology for conquering disease and preventing human suffering. Never before has the right to privacy of health care confronted such peril. Thus, owing to the changing conception of the medical record and its increasing automation, there is a critical need to establish, and where necessary to enforce, public and institutional policies that ensure privacy safeguards for medical records. In turn, this security will contribute to the integrity and efficacy of the physician-patient (or the hospital-patient) relationship.

To a certain extent, the computer may precipitate changes in the traditional physician-patient relationship. The greater participation of subspecialists in patient care requires that more people have access to medical records. Although automation is not responsible for medical specialization, the gathering of scattered medical data into a single computerized medical record may create new problems. The efficiency of an automated system makes violations easier, and the comprehensiveness of the files contained therein leads to more damaging results when violations occur.

The analysis of privacy rights raises three major interrelated issues, including (*a*) sources of a right to

privacy, (*b*) disclosure and uses of medical records, and (*c*) security of medical records and PCMS. Our primary purpose for this paper is to review these issues and to suggest several public and institutional policies that might better protect the privacy and confidentiality of patients in general, with a specific emphasis on hospitals. The ensuing discussion focuses on problems encountered in a clinical, patient treatment environment and does not expound on the additional set of dilemmas encountered in the use of records in medical, epidemiologic, or social research.

Sources of a Right to Privacy

Ethics and professional codes. From an ethical perspective, it is relatively clear that based on the principle of "respect for persons," people have a right to have the confidentiality of their medical records preserved (*20*). Furthermore, according to Kant, this respect for persons, which reflects a freedom of will, is significant in assuring one's autonomy (*21*). Justice Cardozo cited an analogous principle in his well-known 1914 decision (*22*): "Every human being of adult years and a sound mind has a right to determine what shall be done with his body." Since information generated regarding one's mind and body may be viewed as an extension of one's body, the concept of autonomy dictates that one has the option to control the uses of that information.

Clinical practitioners cite the Hippocratic oath, the Principles of Medical Ethics of the American Medical Association (AMA), or their right to "privileged communication" as being more than sufficient to guard their protection of patients' privacy and confidentiality. Physicians commonly maintain that they are bound to protect the information collected in the intimacy of their offices or their patients' hospital rooms. This promise of confidentiality permits patients to speak freely and openly discuss their symptoms without fear that disclosures about their problems may cause personal or public embarrassment or prosecution.

Although not directly engaged in the delivery of clinical services, other health care professionals, such as hospital administrators subscribing to the Code of Ethics of the American College of Hospital Administrators (ACHA) and registered record administrators adhering to the ethical code of the American Medical Record Association (AMRA) also guard the confidentiality of the personal information with which they are entrusted. Such professional organizations have dedicated considerable efforts and resources to the protection of patients' records from unauthorized or inappropriate intrusion, as evidenced in 1977 with the issuance of "Confidentiality of Patient Health Information: A Position Statement of the American Medical Record Association" that addresses many related issues (*23*). This document, which includes a set of model policies for maintaining the confidentiality of medical records and medical record information, was designed to assist health care institutions in formulating their internal policies for assuring the security of medical records. Additionally, the AHA Board of Trustees in November 1978 approved its "Institutional Policies for Disclosure of Medical Record Information," which focuses on the hospital's responsibility to protect patient confidentiality (*24*).

However, violations still occur. What is said to physicians during the course of an examination and followup care is noted in the medical record; often, this information is obtained by credit companies, employers, or insurance brokerages without the knowledge of the patient. The improper collection and use of medical information may have lasting consequences on a person. Evidence from recent congressional inquiries has clearly documented several such breaches of confidentiality (*25,26*).

Although physicians strongly defend their maintenance of patient confidentiality on ethical and professional grounds, they are also obligated to weigh the welfare of the community or their legal or societal obligation and reveal or report certain conditions to the appropriate authority. Such a dilemma was circumscribed in the AMA's "Principles of Medical Ethics" in 1957 (section 9) (*27*):

> A physician may not reveal the confidences entrusted to him in the course of medical attendance, or the deficiencies he may observe in the character of patients unless he is *required* to do so *by law* or unless it becomes *necessary* in order *to protect* the *welfare* of the individual or the community.

With the revision of the AMA's Principles in 1980, the position of physicians subscribing thereto engenders more conflict between their strong adherence to the principle of confidentiality and the societal constraints placed on their actions by law. In a somewhat more ambiguous, less emphatic stand, section 4 of the new code states (*27*):

> A physician shall respect the rights of patients, of colleagues, and of other health professionals, and shall safeguard patient confidences *with the constraints of law.*

The law. Many erroneously believe that any communication between physician and patient is bound automatically by law to be kept confidential because it is privileged. However, privilege is a legal concept; it is a statutory provision based on the patient's right to privacy and confidentiality of consultation that protects the physician from having to testify about medical treatment and the content of all communications

related thereto. A communication is viewed as privileged if the person to whom the information is given is forbidden by law from disclosing it in court (either by testifying or producing a medical record) without the consent of the patient. Hence, privilege applies only to judicial proceedings; it is a legal rule of evidence (*5b,19b*). Although it is a legal right only of the patient, not the physician (*5b*), the typical statutory prohibition against the disclosure of medical-record information by medical professionals is focused on protecting the professional and not the patient. Furthermore, since the physician-patient privilege is binding only in a court of law and in relation to the medical treatment that is the subject of the litigation, it should not be perceived as a general prohibition against the release of patient information by a physician (*28*). For example, if the mental condition of a patient is not the subject of the proceedings, delivery of prior mental health treatment may be revealed.

Since the physician-patient relationship is not recognized as privileged under common law, such as the attorney-client privilege (*5b*), it exists by law to some extent in most States because nearly all have enacted such a statute (*29a*). Thus, confidentiality of the physician-patient relationship enjoys no sweeping legal protection unless by specific State statute (*30*). In the four States where such a law does not exist, privileged communication can be recognized only on a case-by-case basis. No physician-patient privilege is recognized in Federal law (*31*).

Beyond the individual State statutory protections of physician-patient privilege, some States have enacted privacy laws that include private recordkeepers, such as insurance companies and hospitals. Generally, it seems that States have avoided blanket protection, and are awaiting Federal action. The Privacy Protection Study Commission summarized current State laws as follows (*19c*):

> Nineteen states have regulations, statutes, or case law recognizing medical records as confidential and limits access to them. In 21 states, a physician's license may be revoked for willful betrayal of professional secrets. These statutes do not generally apply to medical care providers other than physicians, and although the codes of ethics of most allied health professions reaffirm the principle of confidentiality, the codes can impose only a moral, not legal, obligation.

Since the right of privacy is so cherished, some have argued that is it protected in the U.S. Constitution by provisions of the Bill of Rights, most notably the 1st, 3d, 4th, 5th, 9th, and 14th amendments (*32*). A brief survey of the literature on privacy reveals multiple interpretations and uncertainties (*33*). The common element to all, however, is the noted absence of a firm constitutional statement upon which to pin the privacy concept. The Constitution does not mention the word "privacy," nor does it discuss the privacy concept.

Privacy is considered a reserved right, implicit in a constitutional government that is limited to the exercise of only those powers expressly conferred upon it. The Federal Constitution expresses an interest in privacy, but not a constitutional right to protect it in all situations. It competes with other, sometimes conflicting, constitutional interests such as free speech, freedom of the press, and the public's right to know. However, many aspects of personal privacy have been protected against governmental interference in court decisions through judicial interpretations of the special provisions of the Bill of Rights.

Between 1965 and 1973, several landmark decisions by the U.S. Supreme Court confirmed that the State may not interfere with intimate personal decisions which fall within "zones of privacy" emanating from several constitutional amendments (*34–37*). These significant opinions give substance to privacy arguments, although they have revolved chiefly around debates over contraceptive use and abortion (*38,39*). However, more recent Supreme Court decisions have contributed to a possible retreat from the position upholding the patient's interest in avoiding disclosure of personal medical information. For example, the Court held that a State can require physicians "to record on official forms" information concerning prescriptions for certain potentially hazardous drugs, including the patient's name (*40*). More recently, the Court upheld a Utah law which requires physicians "to notify a minor's parents or guardian" if it is physically possible to do so before performing the minor's abortion (*39,41,42*).

Federal statutes are somewhat broader and specifically address the use and misuse of medical information. In 1967, the Freedom of Information Act (FOIA) mandated disclosures of data maintained in government files, but specifically exempted medical records from such disclosure (*43*). Seven years later, the FOIA was followed by the Privacy Act of 1974 (*44*).

Enactment of the Privacy Act codified, for the first time in American history, principles to protect privacy in the collection and handling of recorded personal information by Federal agencies (*45*). It marked the culmination of many years of public and congressional hearings and investigations of threats to personal privacy by the acquisition of vast quantities of computerized personal data by the Federal Government. Because the Privacy Act applies to all Federal agencies, it includes medical facilities, health insurance, and

payment records (for example, Medicare) maintained by the Federal Government. The act provides guidelines for the collection, maintenance, and use of personal data, including medical records (computerized and manual). Although designed to guard against abuse in the dissemination of private data, the act is limited because of its numerous exceptions.

A major limitation of the Privacy Act is that it does not apply to State or local governments or to private agencies (*46*). Its failure to cover more constitutes a broader policy issue and needs to be addressed. It applies only to systems of records from which information is retrieved by the person's name or by some other identifier (*47*). Access is not granted if information is filed under an organizational name or as aggregate information without the use of a form of personal identifiers. Weaknesses aside, the Privacy Act of 1974 is a landmark. It acknowledged the hazards of uncontrolled collection, storage, retrieval, and exchange of personal information as well as the wrongfulness of not granting people access to their records.

However, the right to control who may gain access to one's medical record is within the State's discretion. According to the law in the 50 States, the medical record is the property of the hospital, not the patient. But this property right has been qualified somewhat, over recent years, largely through judicial interpretation and by some State statutes, such as those in Massachusetts and Connecticut (*48*). While hospitals and other institutional providers retain the right of ownership to the physical record—paper, tape, fiche or film—the information contained therein belongs to the patient.

Although a hospital may assert property rights to patients' medical records, it does not have the legal authority to release those records at will to other parties without having prior consent of the patients (*49*). There are no general statutory provisions pertaining to medical records maintained in private medical or health facilities, other than licensed hospitals and clinics, such as visiting nurse services, drug rehabilitation treatment centers, alcoholism centers, or associations for the blind. In such institutions, professional ethical codes establish the rules and regulations in the absence of law (*50*).

At bottom, the most significant and prevailing source of privacy and confidentiality rights remains the professional codes of ethics rather than the law. While individual State laws may privilege health professional-patient relationships to varying degrees and constitutional arguments and court decisions tend to favor privacy rights, ethical mandates appear to provide the most instrumental force for assuring them. For those not bound by strong ethical codes of practice and high professional standards, no other guarantees can be assumed for the present.

Disclosures and Uses of Medical Records

In the early 1900s, 85 percent of medical care services were provided by physicians, mostly solo practitioners. Today, fewer than 5 percent of health care providers are physicians (*51*). In hospitals, only one-third of the data in the records are entered by attending physicians (*52a*). Much of what is recorded is done by other members of the health care team who contribute to the comprehensive care of the patient. In addition to those engaged in the clinical treatment of patients, the Bureau of Health Manpower of the Department of Health, Education, and Welfare estimated that 53,000 persons were employed in the management and administration of medical records in 1974 (*53*). Beyond this number, untold administrative, business office, and other hospital personnel handle or have access to confidential medical records. In sum, hospital records are routinely available to hospital employees on request; most, not all, of whom are health professionals who need such access to fulfill their jobs (*19d*).

Applicable legal provisions and professional codes of ethics (for example, American Medical Association, American College of Hospital Administrators and American Medical Record Association) restrict disclosure of medical records. Disclosures have been consistently deemed justifiable only if made either in the "best interests of the patient" or to foster a "supervening societal interest." Disclosures of medical data, however, commonly occur for these and other legitimate reasons, including the following:

- public health reporting laws mandating disclosure of a significant number of communicable (or infectious) diseases,
- areas concerning patient consent to release medical information, which often are vague, such as determining competency,
- situations entailing conflicting interests between the patient and society when no consensus exists as to the supervening nature of society,
- situations involving the public's right to know, such as matters regarding key public officials, and
- situations arising during the judicial process in which common law principles apply in the absence of State statutes.

Given the nature of the health care relationship, many health care professionals argue that their discretion in making disclosures is not a significant source of abuse (*19e*). It is the role of the physician and

the hospital to assure that a patient's legitimate expectation of confidentiality is not breached as a consequence of negligence by health care professionals. Although protection of the confidentiality of medical records is properly the responsibility of the health care provider and patient authorization is usually obtained before disclosure, evidence suggests that this safeguard is weak (*19e*). Indeed, dramatic and troubling breaches of medical record security have become public in recent years.

The theft and release of Daniel Ellsberg's psychiatric record, the publicizing of Senator Thomas Eagleton's medical history, and the recent exposure of the Factual Service Bureau—a firm that specialized and was highly successful in obtaining medical record information through subterfuge (*52b*)— are but three examples of breaches of medical record security. The Privacy Protection Study Commission has remarked (*19f*):

> That a firm like Factual Service Bureau (now known as Inner-Facts) could be successful, at least until it came under the scrutiny of the Denver grand jury, appears to have been due in no small measure to the laxity of hospital security measures.

Evidence gained from the Factual Service Bureau case demonstrated that similar problems exist elsewhere. (A comprehensive sampling of abuses by others has been recorded in references 5c, 25, and 54 and by the National Commission on Confidentiality of Health Records, Washington, D.C., and the President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research, Washington, D.C.) Although these cases may be viewed as extreme, Smith (*29b*) asserts that the confidentiality of medical records in general is a myth. He argues that regardless of the existence of ethical codes, professional standards, and even a large number of physicians who are strong protectors of their patients' privacy, "The nature of third-party payments nowadays and the proliferation of computer data banks in the insurance and health industries make confidentiality beyond the control of the practicing physician" (*29c*).

Moreover, the Privacy Protection Commission agrees that with the myriad of reporting requirements the secondary use of medical records produces conflict (*19g*) and ". . . raises the sharpest clash between society's interest in protecting medical confidentiality and its interest in a wide variety of other important functions" (*5d*). For, as Westin further observes (*5d*):

> . . . the outward flow of medical data . . . has enormous impact on people's lives. It affects decisions on whether they are hired or fired; whether they can secure business licenses and life insurance; whether they are permitted to drive cars; whether they are placed under police surveillance or labeled a security risk; or even whether they can get nominated for and elected to political office.

However, the Privacy Protection Study Commission (*19h*) acknowledges that:

> . . . this clash is not easy to resolve or even mitigate. From a privacy protection point of view, however, the confidentiality of the medical care relationship has been seriously eroded and clearly needs to be restored. Simply blocking third party access to medical-record information is not the answer. New balances must be struck, recognizing not only that existing law and public policy on the subject are inadequate but also that many of the gatekeeping and credentialing functions that depend on information derived from medical records are essential.

Since patients cannot control disclosure of their records within an institution, that responsibility must be assumed by the institution. Thus, a combination of voluntary self-regulation by institutions, health care providers, the insurance industry, and the legal profession must be undertaken. Hospitals, in particular, need to take affirmative action to assure that the medical records that they maintain are made available only to authorized recipients. Furthermore, any disclosures to users should be made only on a need-to-know basis (*19i*).

Disclosure of medical records or information for any unauthorized reasons or to unauthorized persons without strict controls on the potential uses and the users of the information risks infringements on the rights of patients. As stated earlier, this is particularly true in light of nonhealth professionals currently engaged in administrative roles in health care institutions. In addition, a plethora of third-parties such as employers, prospective insurers, and educational institutions attempt to gain access to confidential records through questionable or illegitimate means. Weak standards or policies that are difficult or impossible to enforce contribute to the success of such efforts.

In addition to the violations of confidentiality precipitated by weaknesses in authorization procedures, the majority of patients (on whom hospitals and physicians maintain medical records) risk the loss of their confidentiality due to general nonspecific release forms. These forms, which many patients routinely are requested to sign authorizing disclosure of their records, are worded so broadly that they more or less give away all of the patients' right to control the release of information contained therein. Existing evidence suggests that better, more effective measures are needed to protect the confidentiality of records maintained by health care providers by preventing their disclosure to third parties.

The three most common types of disclosure over which patients are more likely to have little or no control include (*a*) disclosure to private and government insurers, (*b*) disclosures for health planning, evaluation, and research, and (*c*) disclosures for purposes totally unrelated to medical care or research. Although some

disagreement exists among privacy advocates, most agree that legitimate uses of data are generated from PCMS. However, serious problems—in terms of limiting those having access to data, those who may disclose them, and those who have an interest in using them—arise because of our failure to define and enforce standards relating thereto. The table summarizes the major current users of medical records and the principal purposes for which the records are used. Moreover, no attempt was made to show in this table the source of the data, that is, who rightfully or wrongfully might have been responsible for data disclosure.

Least disagreement exists with respect to disclosure of medical information among health care providers directly involved in patient care, namely diagnosis and treatment of trauma and disease. In this regard, however, it is not necessary that all health personnel have total access to the patient's medical record. For example, laboratory technologists need access to only certain information kept in the medical record and should be entitled only to that which they justifiably need to know to carry out their designated duties. In an issue closely related to treatment, few object to disclosure of health data to professionals engaged in quality assurance. With an understanding that efforts, such as the medical audit, utilization review, PSRO, and case conferences contribute to better medical care, most acknowledge the legitimacy of using information in this regard.

With respect to secondary disclosure of medical information to those involved in the direct financing of health care, there is general, albeit sometimes provisional, acceptance. Such acceptance of disclosure of medical data to governmental financing agencies, at least those at the Federal level, is partially due to assurances afforded by the Privacy Act (the data collected by the Federal Government in such programs as Medicare cannot be disclosed subsequently to another party). The concern that is voiced about releasing information to non-Federal agencies, and to a lesser extent even to Federal ones, is the risk of subsequent disclosure by the secondary user to another interested party. While there is increased sensitivity regarding disclosure to private interests, such as commercial insurance companies engaged in the payment of claims for policyholders, most acknowledge this practice when prior consent of the patient is obtained. Requirement of patient consent for the release of specified medical data promotes a fuller consumer appreciation of the costs as well as a conscious awareness of the tradeoff inherent in third-party financing of personal health care services.

Another form of disclosure, which may be secondary or tertiary depending in part on whether it is mandatory or voluntary and who actually constitutes the discloser, relates to medical information about which there is a prevailing societal interest. A common example might be the requirement that all medical providers (physicians, clinics, or hospitals) must report certain communicable diseases to a designated public health agency. Although some have voiced strong objection to

Uses of medical records

Categories of use and examples of users	*Examples of uses of information from medical records*
Primary use	
Health care providers, including institutional (hospitals) and individuals (physicians)	Purposes related to treatment; training of health professionals; evaluating quality of care; complying with licensure and accreditation standards; conforming to government regulations; research directed at improvement of diagnosis and treatment; promoting effective and efficient use of health resources
Secondary use	
Payors for services, including private insurance companies (Blue Cross/Blue Shield, the commercials) and government insurance (Medicare and Medicaid)	Substantiating patient claims for payment; claim audits for services and fees; monitoring quality and equality of care rendered to insurees; assessing and controlling costs
Tertiary use	
Health service evaluators; health planners; public health agencies; medical and social research agencies; occupational health and safety agenies	Health planning; allocating scarce health resources; epidemiologic surveillance; occupational health and safety efforts
Other uses	
Employers; educational institutions; law enforcement agencies; credit bureaus; media; judicial system	Determining employment suitability; determining admission to colleges and universities; criminal and civil investigations; determining credit eligibility; creating sensational headlines; assessing legal matters

this invasion of personal privacy, frequently into highly sensitive areas such as sexually transmitted diseases, most agree that disclosures for certain epidemiologic surveillance and control programs are valid "in the public interest." However, patients are still entitled to be duly informed of such practices.

The area of most significant controversy revolves around the tertiary use of disclosed medical information, commonly with patient consent, for research purposes. It is within this category that most public health professionals confront the dilemma of balancing the potential benefits that may be gained through such research against the loss of personal privacy. In view of the known impetus of researchers and the magnitude of social expecations of biomedical technology, what constitutes a level of fair and reasonable sacrifice of privacy and confidentiality for the public good? And, who should decide on such standards and practices? Advocates on both sides of the argument continue to debate, and there is little evidence of successful compromise in the near future.

Meanwhile, Federal intervention to protect human subjects of biomedical and behavioral research has resulted in the evolution of regulations to guide current practices (*55*). Furthermore, the recently established President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research has been charged to investigate problems related to privacy and medical records, among others.

Finally, there is consensus that any disclosure of information from medical records for nonhealth purposes (to other users) represents a clear and unjustifiable violation of privacy and confidentiality unless voluntary (noncoercive) informed consent of patients or former patients has been obtained in advance. In most—if not all—such instances, disclosures for "other uses" (except those resulting from court orders in judicial proceedings) are unethical, illegal, or both.

Security of Medical Records and PCMS

Three problems are closely related to and partly responsible for violations of patient confidentiality and privacy: (*a*) failures or inadequacies of security systems, (*b*) inappropriate and unprofessional discussions about patients by health providers, and (*c*) the wide use of blanket, nonspecific patient authorization forms by many institutions. Custodians of medical records and managers of PCMS must take measures to ensure the protection or personal information not only against deliberate or accidental destruction of data but also against unauthorized access or modification of data. The sensitivity of health and medical information requires the establishment of policies and procedures that will limit access to institutional personnel who legitimately need to see the information. Furthermore, a monitoring system is needed to detect unauthorized use and to impose sanctions against intruders. Procedures should be flexible enough not only to safeguard records from unauthorized disclosure but also to permit their release on the written request of the patient.

Threats to data privacy and confidentiality range from accidental release of information to intentional penetration of a health record data bank system. All system personnel—managers, custodians, users, technicians, and recorders—pose threats to the security of the system. Intrusions may also come from outside the system, for example, from an individual or institution who deliberately attempts to gain unauthorized access to data bank records. Regardless of the levels of safeguards, no system, manual or computerized, is 100 percent secure.

Health care institutions have been negligent in establishing controls governing who has access and for what purposes. The problem is not limited to controlled access. When access is permitted for a specific purpose, in response to a legitimate request, often the entire record is transmitted because this is less costly than extracting only the necessary information (*56*). In an automated system, this situation could be corrected with a small investment in software packages—albeit one which probably will not be made until the ethical implications of current practices are exposed.

Threats to security of data can be blocked by a variety of procedures and techniques. However, even the best-designed system cannot prevent authorized users from browsing or maliciously using accumulated information. Most control measures suggested in the literature focus on control of access to or the centralization of information. The first safeguard, simple and easy to implement, is controlling input into the system. Data acquisition should be "use-related." The release of more than the specifically needed data may contribute to an undesired release of very personal, highly sensitive information. Although such data may be entirely accurate, it may be socially undesirable to disclose, for example, treatment for a venereal disease or a mental disability.

A second safeguard—the prevention of unauthorized access to PCMS—should be the primary objective of access management techniques, such as authorization, identification, codes, passwords, and authentication, to reduce threats from external sources and from those having no legitimate need of access. Unfortunately, such efforts do not prevent the illegitimate use of data by personnel who have legitimate access to the system (*57*).

Hence, safeguarding a health care data system involves two areas of protection—the protection of the system itself and the protection of the confidentiality and privacy of the records contained therein. The risk to personal data increases as data are centralized, as the number of users of the information grows, and as greater volumes of data are shared. Personal privacy should always be a paramount concern (*58*). In the spirit of informed consent, it is possible to provide the patient with choices concerning the release of personal information. Society as a whole benefits from the responsible management of data systems which store personal, sensitive information.

Apart from the intentional or accidental disclosures from more complex PCMS and individualized medical records, serious and damaging invasions of privacy are caused by physicians, nurses, and other health care professionals who simply gossip too much (*29a*). Too often such people are overly anxious to break the news about a well-known patient's condition or about a relatively noteworthy procedure or situation without consulting first with the patient or the family. Too commonly, health providers carelessly discuss patients' conditions at parties, when treating other patients, or in the hospital cafeteria or hallways. It is not unusual, for example, for a physician to tell one patient that another patient was in the week before for such-and-such problem. Furthermore, in a crowded hospital cafeteria one often is told or overhears the outcomes of the morning's complicated surgical procedures or of the major traumas treated in the emergency room. The more controversial or rarer the situation, the more likely one is to hear about it through the grapevine. However, as cited previously, the most frequent breach of confidentiality results from the policies of most health care institutions that mandate patients' signing an authorization for any licensed physician, medical practitioner, or other person to disclose medical information. Thus, in subrogating their rights by complying with such policies, patients give broad consent to others and relinquish considerable control over subsequent disclosures.

The solution of the preceding problems requires collaboration by a number of parties—lawmakers, hospital administrators, health practitioners, and patients—in rational decision making to assure quality care, adequate financing, and confidentiality.

Policy Considerations: a Balancing Act

Privacy issues must be addressed through prudent, ethical public policies that reflect a balance between the need for information flow and the right of privacy. These policies should be formulated through consensus of all parties concerned and govern both manual and computerized systems. Privacy issues cannot be resolved on technical grounds alone. The shaping of public policy is a shared responsibility. The formulation and implementation of public policy regarding this issue requires the input of legislators, government agencies, data users, computer manufacturers, and private citizens. When necessary, other objective consultants, including ethicists, may be used to help clarify complex issues and values.

The privacy issue has become a matter of concern because of the ever-increasing demands for services and information. Personal histories are no longer purely personal. Although most data-gathering activities are intended to achieve socially desirable goals, electronic tracks are left for computer personnel to store, retrieve, analyze, exchange, and transmit data.

Within the broad spectrum of records maintained on individual persons, the medical record is special. Its unique characteristics require careful consideration in the formulation of policies dealing with the right of privacy. The medical record is subjected to greater and stronger demands for the release of information. However, many questions arising over the release of information are not covered by law, court decisions, or regulations. The policies of hospital or other medical care institutions serve as guidelines for making information disclosure decisions. Fundamental to the establishment of any privacy policy is the question of whether people will be regarded as special entities with unique needs or whether they are merely objects of society to be dealt with as such by data keepers to satisfy institutional needs. In other words, health institutions confronted with the choice of releasing patient care information or losing fiscal reimbursement must recognize that the choice has more than simply a fiscal dimension. Breaches of privacy can be avoided by restricting the flow of medical information among health care providers. If this is not the case, policy directives may be written with little regard for confidentiality as an inviolate element of health care practice.

Another consideration is the long-term societal need that appears to conflict with the short-term desire among patients for confidentiality. Vital health and medical information, properly managed in a data system, can enhance efforts to improve general patient care and contribute to medical and health services research. As an information-based society, a public policy on information processing that will ensure the proper circulation of data is needed. However, there must be a clear delineation of policies and practices governing the acquisition, analysis, storage, exchange, and transmission of health care data.

A health data information public policy should balance individual and societal needs and interests, identify the special priorities, and determine the extent to which computer technology will be used within the system. Although industry should not be faulted for embracing new technologies, it must be more responsive to privacy issues. In the absence of public policy there is little to prevent private organizations or government agencies from collecting more information than they need or from exchanging vast quantities of personal data.

No single approach will provide solutions to the social problems inherent in information data systems. However, those who handle personal data are obliged to guard the privacy of the patients' records and to ensure the accuracy and completeness of these records.

If public policy is to safeguard personal privacy and create a standard of fair health information practices, it is essential that certain issues be addressed. Privacy experts agree on the following objectives of the policies.

Patients' needs and interests

- an enforceable qualified right for patients to review and copy records,
- an opportunity for patients to have erroneous entries in their records corrected or amended,
- limitations placed on access to records and files,
- regulations forbidding the collection and recording of unverifiable information,
- a duty of confidentiality in the relationship between all (direct and indirect) health care providers and patients,
- notice given to patients of recordkeeping organizations receiving a subpoena, and
- public procedures specified whereby patients can challenge the contents in their records.

Agency needs and interests

- a defined retention period and provisions for expunging obsolete data,
- authorization to provide relevant abstracts or summaries to organizations having a legitimate claim to information rather than releasing entire medical records,
- enforcing rules for data-sharing practices,
- established standards for identifiers and indexing systems,
- clarification of record ownership,
- policies and procedures to ensure data and system security,
- clear assignment of responsibilities for administration and security to specific individuals,
- designation of one person to be directly responsible for the system, and
- detailed information about the system and the legal consequences of breaches of confidentiality or leakage of information provided to all employees.

Societal needs and interests

- notice to data subjects of the identity of the persons or organizations to whom information is transmitted and the conditions under which such a transfer is conducted,
- an enforceable code of conduct for data collectors and keepers,
- a policy of informed consent governing secondary and tertiary use of records, accompanied by a dated, witnessed, signed authorization for the release of a record,
- implementation of a complete and accurate system of access, entries, uses, corrections, deletions, and other modification of the record,
- public notice describing the system, and
- established procedures for reporting data to funding sources in which the identities of patients are not divulged.

Good judgment and self-regulation of the information-gathering and -using agencies are obligations. The privacy of the people to whom benefits and services are rendered must be protected. Intrusions of personal privacy occur every time a person is required to furnish more information than needed, when these data are subsequently reused for unrelated secondary purposes, and when such uses violate promises of confidentiality. While computers provide many advantages, they should not further dehumanize the practice of medicine. Rather, they should be used as tools for improving patient management (*59*).

From a public policy perspective, an ethical framework should be constructed that will permit the exploitation of the advances in computer technology and the manipulation of information for individual and societal benefit while assuring that no one is treated unfairly or harmed by a record system (*60*). For the question is not whether computer technology will be used in the coming decade of medical practice, but rather, how and how much. Basic privacy rights cannot be allowed to become a casualty of technology. To allow this to occur is to abrogate social responsibility.

Not all of the identified issues are, however, exclusively in the realm of public policy, per se. Many are best resolved, at least on an ad hoc basis, by individual health care institutions that have developed mechanisms to evaluate considerations involving patient, agency, and societal needs and interests. The need for such an approach increases as automated medical

record systems merge with the financial and business systems (management information systems) of health care institutions, and third-party payers increasingly claim a need for more and greater detail concerning financial transactions.

Guidance in establishing adequate safeguards to maintain patient privacy and confidentiality have been circumscribed by the Joint Commission on Accreditation of Hospitals (JCAH) in its "Accreditation Manual for Hospitals" (*61*). With respect to patient rights to privacy and confidentiality, JCAH considers the following reasonably applicable to all hospitals (*61a*):

> The patient has the right, within the law, to personal and informational privacy, as manifested by the right to:
> • refuse to talk with or see anyone not officially connected with the hospital, including visitors, or persons officially connected with the hospital but who are not directly involved in his care.
> • expect that any discussion or consultation involving his case will be conducted discreetly, and that individuals not directly involved in his care will not be present without his permission.
> • have his medical record read only by individuals directly involved in his treatment or the monitoring of its quality, and by other individuals only on his written authorization or that of his legally authorized representative.
> • expect all communications and other records pertaining to his care, including the source of payment for treatment, to be treated as confidential.

Although these excerpts from the Accreditation Manual's section on "Rights and Responsibilities of Patients" reflect an acknowledgement by the hospital industry of its need to ensure the privacy of patients, including their medical records, JCAH fails to mandate such an institutional policy or to provide a mechanism for its enforcement by translating this right into a "standard" measured during its formal accreditation process. However, while not including privacy as a general standard, JCAH has taken a critical step toward assuring institutional responsibility to protect patient confidentiality beyond the scope of legal requirements and individual ethical codes of the health professions. Furthermore, with respect to medical records collected and maintained by hospitals, JCAH has established a more specific and formal policy codified into Standard III of the Manual's section on "Medical Record Services" (*61b*): "Medical records shall be confidential, secure, current, authenticated, legible, and complete." Hence, although the intent of protecting the confidentiality of medical record information is clear, the extent to which individual institutions go to assure and uphold confidentiality varies. Moreover, JCAH interpretation of Standard III allows for considerable latitude among institutions in determining which hospital (or nonhospital) personnel may be granted access privileges to medical record information or to whom such information may be disclosed. According to JCAH interpretation (*61b*):

> The medical record is the property of the hospital and is maintained for the benefit of the patient, the medical staff, and the hospital. It is the hospital's responsibility to safeguard both the record and its informational content against loss, defacement, and tampering, and from use by unauthorized individuals . . . Written consent of the patient or his legally qualified representative is required for release of medical information to persons not otherwise authorized to receive this information. This shall not be construed to require written consent for use of the medical record for automated data processing of designated information; for use in activities concerned with the assessment of the quality and appropriateness of patient care; for departmental review of work performance; for official surveys for hospital compliance with accreditation, regulatory, and licensing standards; or for educational purposes and research programs. There should be a written hospital and medical staff policy that medical records may be removed from the hospital's jurisdiction and safekeeping only in accordance with a court order, subpoena, or statute. Any other restrictions on record removal shall be in addition to this basic requirement.

In addition, as noted, in a variety of situations "written consent for use of the medical record" is not required, including its inclusion in PCMS for which JCAH offers no security standards. Also, while JCAH acknowledges the need for and the value of an overall quality assurance program, necessary requirements and mechanisms to ensure the confidentiality of patient records are not specified for accreditation purposes as they should be. Hence, JCAH accreditation standards —which could provide an important vehicle for assuring patient privacy—constitute a weak step, albeit one in the right direction. Subsequent efforts need to strengthen the pivotal role that JCAH could have, particularly amid the increasing demand for automated, sophisticated record systems.

Summary and Conclusions

In providing privacy safeguards without abrading the legitimate interests of data keepers, it is necessary to formulate sound policies that (*a*) define situations under which medical information is disclosed to other parties, (*b*) provide procedures by which patients may gain access to their own records, (*c*) determine ownership of records, (*d*) ensure anonymity in aggregating data for research or statistical purposes and (*e*) carefully balance society's long-term goals and the legitimate need of organizations to use medical record information with patients' short-term desire for and right to privacy.

Balance is needed—making available to society the benefits of medical science and research while at the same time making certain that privacy and confidentiality rights are protected. To achieve this balance, computerization of health data must protect the rights of patients to limit information flow about themselves (privacy) and respect the duty of physicians to restrict the information flow (confidentiality). Even when people disclose personal information in order to re-

ceive health services, they maintain a continuing interest in this information beyond its original disclosure. Patients should be able to exercise some control over their records, particularly since these records are so commonly available to third parties. Patients' authorization, in the spirit of informed consent, coupled with personal access to their records offer some protection against misuse, abuse, and inaccuracies. To this end, records need not be kept indefinitely; procedures should be available by which records can be expunged in part or in their entirety except where continuity of patient care is still relevant and desirable or where an overriding societal benefit for retaining them is demonstrated.

Privacy is a multidimensional problem. While generally in consonance with other rights, it has introduced stress between society and technology. There is a responsibility to share ideas and facts contained in record-keeping systems in an effort to advance education, research, and knowledge. There is a personal right to be left alone, to be autonomous, and to have a right to self-determination. And, there is a collective right to ensure the accountability of health professionals, hospitals, and government.

Obligations, legal and social, sometimes require the disclosure of medical data for such purposes as solving medical and public health problems, preventing occupational hazards, conducting medical research, and evaluating health programs. Furthermore, as health care systems are reshaped to respond to government mandates and societal demands for services, they will make increased use of computer and information technologies. The conversion from manual to automated systems has led generally to a tendency to collect more information, to share and exchange information, and for more people to have access to records. All of these highlight the many difficulties in safeguarding PCMS as there are increasing interests in and more points of access to them. There must be more sophisticated surveillance than that which existed before the proliferation of computers and accompanying technology.

It is therefore incumbent on professional associations (such as the AMA, AMRA, ACHA) and other organizations, particularly those carrying licensing and accrediting authority (for example, the JCAH) to enforce voluntarily imposed standards based on ethical values. Existing evidence suggests that the recent trend toward promoting privacy and confidentiality rights has been positive, despite certain pockets of opposition; however, much remains to be done.

The nature of health information requires an environment that preferentially encourages the development of a desirable system. Laws pertaining to the issue of privacy are just in their infancy. This situation presents opportunities for health care professionals and institutions to contribute to the creation of their own codes of ethics and the formulation of rules and regulations to protect privacy.

Restrictions must be placed on the contents and release of personal information. Without adherence to voluntarily imposed ethical standards, the alternative will force further promulgation, implementation, and enforcement of stricter legal sanctions. If future laws restrict the use, amount, and type of data to be extracted from people, there will be constraints on the delivery of services. Nonetheless, such restrictions will create an environment that enables people to exercise their right to privacy and confidentiality.

Editor's note: Substantial portions of this paper were published as "Computers, Medical Records, and the Right to Privacy," by Marc D. Hiller and Vivan Beyda, in the Journal of Health Politics, Policy and Law, Vol. 6, No. 3, pp. 463–487, fall 1981.

References

1. Harris, D. K., and Polli, G. J.: Computers and medicine: special report. American Medical Association, Chicago, 1979, p. 2.
2. Opp, M.: The confidentiality dilemma. Mod Health Care 5: 52, May 1975.
3. Bekey, G. A.: Retrospect and overview. *In* Hospital information systems, edited by G. A. Bekey and M. D. Schwartz. M. Dekkerm, New York, 1972, p. 391.
4. Hodge, M.: Medical information systems: a resource for hospitals. Aspen Systems Corporation, Germantown, Md., 1977.
5. Westin, A. F.: Computers, health records, and citizen rights. National Bureau of Standards Monograph No. 157. U.S. Government Printing Office, Washington, D.C., December 1976; (*a*) p. 308, (*b*) p. 21, (*c*) pp. 219–245, (*d*) p. 60.
6. Data security systems—threats and deficiencies in computer operations. Translated from IBM Svenska Publication No. G320–5646. International Business Machine Corp., White Plains, N.Y. 1975.
7. Niblett, G.: Digital information and the privacy problem. Organization for Economic Cooperation and Development, Paris, 1971.
8. Younger, K.: Report of the committee on privacy. Her Majesty's Stationary Office, London, 1972.
9. Commission on Human Rights: Human rights and technological developments: use of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society. Publication No. E/CN. 4/142 English. United Nations, Geneva, January 1974.
10. Pentages, A., and Pipe, G. R.: A new headache for international DP. Datamation 23: 115–126, June 1977.
11. Confidentiality, records, and computers. Brit Med J: 698–699, Mar. 10, 1979.
12. Hewitt, P.: Computers, records, and the right to privacy. Input Two-Nine Ltd., Surrey, United Kingdom, 1979.
13. Warren, S. D., and Brandeis, L. D.: The right to privacy. Harvard Law Rev 5: 193–219, December 1980.

14. Davis, R.: Government looks at: privacy and security in computer systems. Computer and Business Equipment Manufacturers Association, Washington, D.C., 1973.
15. Curran, W. J., Sterns, B., and Kaplan, H.: Privacy, confidentiality, and other legal considerations in the establishment of centralized health data system. N Engl J Med 281: 243, July 1969.
16. U.S. House of Representatives, Committee on Government Operations: Right to privacy proposals of the Privacy Protection Commission. Hearings. 95th Cong., 2d sess. U.S. Government Printing Office, Washington, D.C., 1978.
17. Hiller, M. D., and McHugh, M. J.: Patient rights: an advocate's perspective. J Am Coll Health Assoc 27: 124–129, 138, December 1978.
18. Preyer, R.: Federal privacy of information act. Congressional Record, Nov. 16, 1979, p. H10964.
19. Privacy Protection Study Commission: Personal privacy in an information society: the report of the Privacy Protection Study Commission. U.S. Government Printing Office, Washington, D.C., July 1977; (*a*) p. 533, (*b*) pp. 283–284, (*c*) p. 284, (*d*) p. 285, (*e*) p. 305, (*f*) p. 285, (*g*) p. 281, (*h*) pp. 281–282, (*i*) p. 304.
20. Lebacqz, K., and Levine, R. J.: Respect for persons and informed consent to participate in research. Clin Res 25: 101–107 (1977).
21. Kant, I.: Fundamental principles of metaphysics of morals. *In* Selections, edited by T. M. Greene. Charles Scribner's Sons, New York, 1929, p. 234.
22. *Schloendorff* v. *Society of New York Hospital,* 211 N.Y. 125, 129–130; 105 N.E. 92, 93 (1914).
23. American Medical Record Association: Confidentiality of patient health information: a position statement of the American Medical Record Association. Chicago, 1978.
24. American Hospital Association: Institutional policies for disclosure of medical record information. Chicago, 1978.
25. U.S. Senate, Committees on Government Operations and the Judiciary: Privacy: the collection, use, and computerization of personal data, pt. 1. Hearings. 93d Cong., 2d sess. U.S. Government Printing Office, Washington, D.C., 1974.
26. U.S. House of Representatives, Committee on Government Operations: Privacy of medical records. Hearings. 96th Cong., 1st sess. U.S. Government Printing Office, Washington, D.C., 1980, pp. 1129–1140.
27. American Medical Association: Principles of medical ethics. Chicago, 1957; revised 1980.
28. Brant, J., Garlinger, G., and Brant, R. T.: So you want to see our files on you. *In* Children's rights and the mental health professions, edited by G. P. Koocher. John Wiley and Sons, New York, 1976, p. 124.
29. Smith, R.: Privacy: how to protect what's left of it. Anchor Press/Doubleday, Garden City, N.Y., 1980; (*a*) p. 128, (*b*) pp. 127–144, (*c*) p. 127.
30. Curran, W. J.: Protection of privacy and confidentiality. Science 182: 797 (1973).
31. O'Sullivan, A. L.: Privileged communication. Am J Nurs 80: 947–950, May 1980.
32. Parker, R. B.: A definition of privacy. Rutger's Law Rev 27: 275–296, winter 1974.
33. Gavison, R.: Privacy and the limits of law. Yale Law Rev 89: 421–471, January 1980.
34. *Griswold* v. *Connecticut,* 381 U.S. 479 (1965).
35. *Eisenstadt* v. *Baird,* 405 U.S. 438 (1972).
36. *Roe* v. *Wade,* 410 U.S. 113 (1973).
37. *Doe* v. *Bolton,* 410 U.S. 179 (1973).
38. Wing, K. R.: The law and the public's health. C. V. Mosby Company, St. Louis, 1976, pp. 55–69.
39. Curran, W. J., and Shapiro, E. D.: Law, medicine, and forensic science. Ed. 3. Little, Brown and Company, Boston, 1982, pp. 883–935.
40. *Whalen v. Roe,* 429 U.S. 589 (1977).
41. *H.L.* v. *Matheson,* 604 P.2d 907 (Utah 1979); *H.L.* v. *Matheson,* 49 U.S.L.W. 4255 (No. 79-5903).
42. Alan Guttmacher Institute: Parental notice for abortion upheld in some cases. Family Plann/Pop Reporter 10: 17–18, April 1981.
43. 5 U.S.C. 552 (1967).
44. Public Law 93–579; U.S.C. 522a (1974).
45. Weekly compilation of presidential documents, vol. II, pt. 1. U.S. Government Printing Office, Washington, D.C., 1975, p. 7.
46. U.S. Senate, Committee on Government Operations: A citizen's guide on how to use the privacy act in requesting Government documents. 95th Cong., 1st sess. U.S. Government Printing Office, Washington, D.C., 1977, p. 5.
47. Beverage, J.: The privacy act of 1974: an overview. Duke Law J 1976: 303, May 1976.
48. Meyer, J.: Re: patients' right of access to medical records—summary of the law. New Hampshire Civil Liberties Union. Concord, 1980. [Typewritten opinion submitted to Marc D. Hiller.]
49. Getman, W. H.: Access to medical and psychiatric records: proposed legislation. Albany Law Rev 40: 580–617, May 1976.
50. Kaiser, B. L.: Patients' right of access to their own medical records: the need for a new law. Buffalo Law Rev 24: 317–330, winter 1975.
51. Freeman, A.: Protection of sensitive medical data, patient-centered health systems. Society for Computer Medicine, Minneapolis, 1975.
52. Privacy Protection Study Commission: Medical records. Hearings, June 10, 1976. U.S. Government Printing Office, Washington, D.C., 1976; (*a*) p. 84, (*b*) p. 474.
53. U.S. Department of Health, Education, and Welfare: The supply of health manpower. U.S. Government Printing Office, Washington, D.C., 1974, p. 144.
54. Grossman, M.: Confidentiality and third parties. American Psychiatric Association, Washington, D.C., 1975, pp. 53–59.
55. U.S. Department of Health and Human Services: Final regulations amending basic HHS policy for the protection of human research subjects, Federal Register 46: 8366–8392, Jan. 26, 1981.
56. Levine, C.: Sharing secrets: health records and health hazards. Hastings Center Rep 7: 13–15, December 1977.
57. Springer, E.: Automated medical records and the law. Aspen Systems Corporation, Rockville, Md., 1971.
58. Jackson, C.: Guardians of medical data. Prisms 2: 43 (1974).
59. Ryan, G., and Monroe, K.: Computer assisted medical practice: the AMA's role. American Medical Association Center for Health Services Research and Development, Chicago, 1971.
60. Ware, W.: Public policy aspects of an information age. Rand Corporation, Santa Monica, Calif., 1977, p. 9.
61. Joint Commission on Accreditation of Hospitals: Accreditation manual for hospitals, 1981 edition. Chicago, 1980; (*a*) pp. xiii–xvi, (*b*) p. 88.