PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION

FOREWORD

The Clinton administration's health care reform proposal, announced by the President on September 22, 1993, places substantial reliance on telecommunications and information technology to reduce costs and improve health care delivery. By linking computerized health information through a national network, the proposal envisions a system that would allow an efficient exchange of information to improve patient care and expand resources for medical research and education, while lowering health care costs. While automation may or may not achieve these goals, it will raise serious questions about individual privacy and proper use of the health care information system. This report analyzes the implications of computerized medical information and the challenges it brings to individual privacy.

In its analysis, the report examines: 1) the nature of the privacy interest in health care information and the current state of the law protecting that information; 2) the nature of proposals to computerize health care information and the technologies available to both computerize and protect privacy in the information; and 3) models for protection of health care information.

This study was requested by the Senate Subcommittee on Federal Services, Post Office, and Civil Service, and the House Subcommittee on Government Information, Justice, and Agriculture. The Subcommittees asked the assistance of the Office of Technology Assessment in confronting the issue of confidentiality of health care information in a fully automated medical environment. OTA drew upon the contribution of participants at two workshops, and received valuable assistance from officials of the U.S. Department of Health and Human Services, the National Institute of Standards and Technology, the French Ministry of Health and the European Economic Community, as well as a broad range of individuals and professional organizations from the medical community, public interest groups, industry, and academia.

OTA appreciates the participation of the advisory panelists, workshop participants, Federal agency officials, and interested citizens, without whose help this report would not have been possible. The report itself, however, is the sole responsibility of OTA.

ROGER C. HERDMAN, Director

Program Ref: Industry, Telecommunications, and Commerce Program

CONTENTS

1 INTRODUCTION, SUMMARY, AND OPTIONS

Computerization of health care information, while offer ing new opportunities to improve and streamline the health care delivery system, also presents new chal lenges 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.

1.1 BACKGROUND AND STUDY APPROACH

Previously, the Office of Technology Assessment has ex plored the need to protect the confidentiality and integrity of data and information that is processed and transmitted using communications and computer technology. (See footnote 1) OTA's objectives for this study were to:

- 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 informa tion system security; government agencies; and public interest groups. This was accomplished through interviews, correspondence, and public participation in two workshops. (See footnote 2)

OTA explored the issue of privacy in comput erized medical information by addressing ques tions 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 limita tions 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 in formation 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?

1.1.1 What Is Health Care Information?

The Institute of Medicine report, The Computer- Based Patient Record: An Essential Technology for Health Care (see footnote 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 1-1). 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. (See footnote 4) Parties who are not directly involved in patient care also gather and maintain health care information, and are often referred to as second ary 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, (see foonote 5) rehabilitation and social welfare programs, credit agencies and banking centers, public health agencies, and medical and social researchers (see figure 1-2).

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's 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.

1.2 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.

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. (See footnote 6) (For adiscussion of the distinction between the terms "privacy" and "confidentiality" and for definitions of these terms for purposes of this report, see box 1-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 healthcare delivery by providing resources for medical research. The lack of proper protections for privacy could lead to (and has, in some cases) the physician's withholding 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. (See footnote 7) Safeguards to privacy in individual health care information are imperative to preserve the health care delivery relationship and the integrity of the patient record.

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. (See footnote 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 for ward, OTA did not analyze the question of whether computerization of patient information is appropriate to the interests of individual privacy.

1.3 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, how ever, computer systems for patient information have been largely associated with medical centers, hospitals, or offices. Departments within 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 data bases, decision support tools and reliable transmission of detailed information across substantial distances." (See footnote 9)

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 providers and at various health care sites. (See footnote 10) This would provide a longitudinal record, one that forms a cradle-to-grave view of a patient's health care history. (See footnote 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 (see footnote 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 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 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. (See footnote 13) (For a discussion of the privacy challenges presented by online systems and smart card systems, see box 1-B). Some are concerned that individuals may not even know the content of the information they are carrying on the card. (See footnote 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. (See footnote 15)

1.3.1 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 confidentiality measures, employee education, and personnel and confidentiality policies.

1.3.2 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. Supple menting 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.

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 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.

1.4 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 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 specifically by the Federal Government. The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment.

1.4.1 Ethical Sources

The physician's (see footnote 16) confidentiality obligation can be found in the Oath of Hippocrates, written between the Sixth Century B.C.E. and the First 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 second ary 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.

1.4.2 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 (see footnote 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 further discussion of the Supreme Court's analysis of a right to privacy, see box 2-B).

1.5 FEDERAL LAW

While some Federal laws address the question of privacy in certain information collected and maintained by the Federal Government, no Fed eral 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 (see footnote 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 require ments 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 Health and Human Services, except as prescribed by regulation.

1.6 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 stand ards 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.

1.6.1 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 new problems. 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:

- 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. (See footnote 19)
- The computer's ability to transmit large volumes of data instantaneously make the potential dissemination of medical information 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.

1.7 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 (see footnote 20)–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.

1.7.1 The Unique Patient Identifier

Proponents of computerized medical information recommend the use of a unique patient identifier to be assigned to a patient at birth and remain permanently throughout the patient's 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. (See footnote 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 should be carefully considered before it is used for that purpose.

1.7.2 Informed Patient Consent to Information Disclosure

Because computerization of medical informa tion 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 gaining 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.

1.7.3 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.

1.7.4 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 provid ers' systems and databases. In addition to link ages 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.

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.

1.8 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 determin ing what information about them is in a record and how it is used.
3. Individuals must have a means of prevent ing 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 disagree ment, 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 develop ment 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.

1.9 CONGRESSIONAL OPTIONS

As computerization of patient records goes forward, Federal legislation is necessary to address issues of patient confidentiality and privacy. (See footnote 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 1a. 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 Federal (see footnote 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 located in different States and operating under different State laws.

If not modified, the present patchwork of laws regarding patient health care information will likely require that resolution of issues of individ ual privacy and improper use of medical informa tion 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 1b. 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 recourse 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 infor mation, amendment, correction and dele tion of information, and creation of data bases;
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, (see footnote 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 data bases 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. (See footnote 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 neces sary to protect individual privacy.

1.10 FOOTNOTES

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 Systems 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-310 (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.

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.

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.

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).

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

10 Ibid.

11 Ibid., p. 45.

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

13 Criticism of the smart card approach stems largely from the proposal that such a system involves 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.

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

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

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

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.

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

23 Federal law protects privacy 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.

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 countries, 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.

2 THE RIGHT TO PRIVACY IN HEALTH CARE INFORMATION

The report of the Institute of Medicine (hereafter referred to as "the IOM report"), claims that computers, high-performance networks, and technologies that allow electronic storage, transmission, and display of medical images will improve the quality of patient care, advance the science of medicine, lower health care costs, and enhance the education of health care professionals. The IOM study cites ways in which computerization of patient records could improve the quality of patient care by offering a way to improve the ease of access to patient care data. Computerized patient records could facilitate integration of patient information over time and from one care provider to another. They could make medical knowledge more accessible to practitioners, and they could support decision making by practitioners. (See footnote 1) With respect to medical research, the IOM report states that computerization could improve data and access to data by researchers, and research findings could be provided to practitioners over medical information computer systems. (See footnote 2)

Computerization is seen also as a way to assist in lowering health care costs. The IOM report argues that improved information could reduce redundant tests and services carried out when test results are not available to the practitioner. Administrative costs could be reduced by electronic submission of claims and the ability to generate reports automatically. Practitioner productivity could be improved in three ways:

- reduce the time required to find missing records or to wait for records already in use,
- reduce the need for redundant data entry, and
- reduce the time needed to enter or review data in records. (See footnote 3)

The Computer-based Patient Record Institute (CPRI), an organization of public and private sector entities concerned with the computerization of patient records, was established in response to a recommendation of the IOM report. (See footnote 4) Its purpose is to facilitate development, implementation, and dissemination of the computer-based patient record, and its vision is the use of a comprehensive, longitudinal patient record to provide all clinical, financial, and research data. The computer-based patient record would contribute to more effective and efficient care through:

- access to lifetime health data collected and contained across the continuum of care;

- support for quality of health care delivery;
- ready access to knowledge bases to support clinical practice, administration, education, and research;
- patient participation in health status determina tion; and
- wellness and disease prevention.

The Workgroup for Electronic Data Interchange (hereafter referred to as "WEDI") 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. According to its report, such a system could reduce administrative and health care delivery costs. Electronic process ing of insurance and managed-care administrative transactions, such as claims, eligibility checks, and coordinating benefits, could streamline pay ers' operations and reduce the administrative tasks of providers. Clinical applications, such as computerized patient records, test results, and outcome studies, might assist providers in ensuring high-quality care without unnecessary or duplicate procedures. (See footnote 5)

While endorsing the adoption of the computer- based patient record and electronic data interchange for health care, these reports acknowledge the concerns about privacy that such systems raise. The IOM study notes that, "the computerization of most types of record keeping, as well as the recent well-publicized cases of inappropriate access by computer hackers, has increased concerns about the misuse of personal information." (See footnote 6) Among the concerns cited by the IOM study are security features of computer-based patient record systems, the lack of generally accepted standards for protection of computer-based medical data across States, and the potential for invasion of patient privacy presented by a personal identification number for all patient records.

The Report of the Work Group on Computerization of Patient Records to the Secretary of the U.S. Department of Health & Human Services (see footnote 7) echoes the concerns of the IOM study. The Work Group on Computerization Report asserts that linkages between systems will significantly enhance access to patient information, thereby offering tremendous potential for improving the quality and efficiency of health care delivery. With enhanced access, however, come concerns about confidentiality and the protection of patient privacy. While patient data is already shared among those who deliver and pay for care, the health information infrastructure envisioned by the Work Group on Computerization Report would make patient information accessible to care givers, payers, and others, and would create new opportunities for abuse unless protection for patient privacy is built into its design and use.

The WEDI Report discusses in depth the serious implications for privacy raised by the use of computer databases linked electronically for information exchange. The report clearly states that:

> [t]he electronic technology itself holds intrinsic threats to maintenance of personal privacy. The same technology that made it possible to transmit data from one computer to another, whether those computers are in the same room or on opposite sides of the globe, also permits violations of data integrity and data security.

It goes on to assert that:

> [t]he establishment of the types of data repositories envisioned for health care claims processing to effect administrative savings should be accompanied by promulgation of significant patient rights regarding the accuracy of personal information maintained and the extent to which it is shared with others. The need for security and confidentiality of patient information should not be subject to individual organizational determination of need. Security and confidentiality must be preserved and protected. They must not be compromised for expedience or the "bottom line."

The WEDI Report examines the complex state of the law regarding privacy and confidentiality in such information, and cites the need to streamline the protection of patient information as one of the key steps the industry must take to implement electronic data interchange efficiently. Recent surveys demonstrate that the concerns voiced in these reports reflect a broad concern among the American public about privacy in their personal information. A joint Lou Harris/Equifax survey indicated that 79 percent of Americans feel their personal privacy is threatened, and some segments of the population fear that consumer information will be more vulnerable by the year 2000. Most Americans also specifically acknowledge the dangers to privacy of present computer uses. According to the survey, two-thirds of the public believes that personal information in computers is not adequately safeguarded, and a significant portion of the American public no longer has confidence in the way industry treats personal information. Almost 9 of 10 Americans surveyed believe that computers have made it much easier for someone to improperly obtain confidential personal information about individuals. (See footnote 8)

In an earlier poll, conducted by Time and CNN in 1991, 93 percent of respondents asserted that companies that sell personal data should be required to ask permission from individuals in advance. California's Privacy Rights Clearing house, the first privacy hotline in the Nation, logged more than 5,400 calls within 3 months of its inception in November 1992. (See footnote 9)

These concerns are well founded. A market exists for the sale of personal information from both public and private sources, encouraged by financial incentives for staff to supplement their income through unauthorized disclosures of personal information. Prosecutions of U.S. Federal Government employees for unlawful disclosure of personal information indicate the risk of invasion of privacy perpetrated by trusted insiders. Those indicted include current or former employees of the Social Security Administration, the Internal Revenue Service, local police officers accessing the FBI's National Crime Information Center, and a number of information brokers. In most of these instances, employees were bribed by information brokers and private investigators representing private clients. (See footnote 10) Anecdotal evidence in this country, and formal investigative work overseas, indicates that abuse of information, and specifically medical information, is widespread. (See boxes 2-A, 2-B, and 2-C)

In addition, increasingly interconnected, affordable, fast, online systems enable the building of electronic dossiers. Macworld magazine reported that it investigated 18 business leaders, politicians, Hollywood celebrities, and sports figures, primarily in the State of California where most public records are online. The investigation sought all legally accessible data available from four commercial and two governmental data suppliers. Investigators were able to obtain the following kinds of information: birth dates, home addresses, home phone numbers, social security numbers, neighbors' addresses and phone numbers, driving records, marriage records, voter registration, biography, records of tax liens, campaign contributions, vehicles owned, real estate owned, commercial loans and debts, civil court filings, corporate affiliations, public records for criminal court filings, fictitious business names, records of bankruptcies, insider trading transactions, trusts, deeds, and powers of attorney. To obtain this information, investigators spent an average of only $112 and 75 minutes per subject. (See footnote 11)

2.1 WHY IS PRIVACY IN HEALTH CARE INFORMATION IMPORTANT?

Health care information relates to profoundly personal aspects of an individual's life. The medical records kept by physicians and hospitals about patients may include identifying information, x-ray films, EKG and lab test results, daily observations by nurses, physical examination results, diagnoses, drug and treatment orders, progress notes and post-operative reports from physicians, medical history secured from the patient, consent forms authorizing treatment or the release of information, summaries from the medical records of other institutions, and copies of forms shared with outside institutions for insurance purposes. But in addition to objective observations, diagnoses, and test results, medical records may also contain subjective information based on impressions and assessments by the health care worker. Medical records may also include impressions of mental abilities and psychological stability and status; lifestyle information or suppositions (including sexual practices and functioning); dietary habits, exercise and recreational activities (including dangerous ones life insurers would want to know about); religious observances and their impact on treatment decisions; alcohol and drug use; and comments on attitudes toward illness, physicians, treatments, compliance with therapy and advice, etc. (See footnote 12) Staff comments about the patient's character or demeanor are sometimes included in the record. Increasingly sophisticated diagnostic tools yield more and more detailed, and potentially sensitive information about a person's body–genetic research and testing results in information that not only indicates a patient's present condition but also enables prediction of his or her future medical condition and the prospect of developing specific medical problems.

Medical information can affect such basic life activities as getting married, securing employment, obtaining insurance, or driving a car. (See footnote 13) Medical conditions have served as the basis for discriminatory practices, making it difficult to participate in these activities. (See footnote 14) Because of its highly sensitive nature, improper disclosure of medical information can result in loss of business opportunities, compromise to financial status, damage to reputation, harassment, and personal humiliation. However, defining what is "sensitive" in a record may be difficult, since the definition may depend on the intended use of a record. (See footnote 15)

Yet at the same time, the integrity of the patient record and the disclosure by the patient to the physician of information necessary to establish an accurate diagnosis is desirable to attain the best clinical outcome. Simply stated, disclosure of medical information by the patient, free of the fear of improper disclosure, is necessary to obtaining good quality medical care. An environment must be maintained in which this kind of disclosure is possible. In its testimony to the U.S. Privacy Commission, the American Medical Association stated, "Patients would be reluctant to tell their physicians certain types of information, which they need to know in order to render appropriate care, if patients did not feel that such information would remain confidential." (See footnote 16) More recently, the AMA Code of Medical Ethics stated:

The confidentiality of physician-patient communications is desirable to assure free and open disclosure by the patient to the physician of all information needed to establish a proper diagnosis and attain the most desirable clinical outcome possible. Protecting the confidentiality of the personal and medical information in such medical records is also necessary to prevent humiliation, embarrassment, or discomfort of patients. At the same time, patients may have legitimate desires to have medical information concerning their care and treatment forwarded to others. (See footnote 17)

2.2 UNREGULATED COMPUTERIZATION AND MARKETING OF HEALTH CARE INFORMATION

In addition to the widespread problem of information brokering and abuse of authorized access to computerized information within a large public sector database of sensitive information, the private sector has begun now to respond to a strong commercial incentive to aggregate medical information. In some instances, such as that of the Medical Information Bureau, (see footnote 18) information is gathered and banked solely for the purpose of assisting the insurance industry in making coverage exclusions in their policies. In other cases, companies offering such computer services as health insurance claims processing, office management, or patient billing, take advantage of their access to medical information (see box 2-D). In these instances, aggregate information is gathered and sold, usually without patient knowledge or consent. At this time, there is no law prohibiting these practices. (See footnote 19) The businesses involved in these ventures operate under no regulatory guide lines regarding security measures, employee practices, or licensing requirements.

2.3 POTENTIAL FOR INCREASED DEMANDS FOR COMPUTERIZED INFORMATION

The IOM study discusses in some detail the increasing demand by multiple users for access to patient care data. (See footnote 20) According to the report, information must be shared among many professionals who are involved in delivery of health care. In addition to these persons, administrators and managers of health care institutions require information to monitor quality of care and allocate resources. To develop budgets, measure productivity and costs, and assess market position, managers of institutions seek to link financial and patient care information.

Quality assurance activities also involve access to information. Among those organizations involved in such activities are the Joint Commission on Accreditation of Healthcare Organizations (JCAHO). Third party payers carry out quality monitoring and evaluations. The best known is perhaps the Medicare peer review organization program administered by the Health Care Financing Administration. Increased Federal involvement in health care has resulted in greater need by the government for medical information. Programs that pay for health services legitimately require review of individual medical information as part of the payment process. In 1992, Medicare alone paid over $ 126 billion for health services. (See footnote 21)

Related programs for quality control and to limit fraud, abuse, and waste have needs for medical records. In addition, records are maintained by agencies that operate health programs such as the Department of Veterans Affairs, the

Department of Defense, Indian Health Service, and the Public Health Service. (See footnote 22)

Demands for information come not only from review bodies, third-party payers, outside billing and computer services, and government, but also from employers, insurers, and others who use health care information for nonhealth purposes. Some suggest that, as the supply of computerized personal medical information increases, there may be a demand for access to information that is not currently authorized. Will investors seek "medical reports" on the chief executive officers of companies in which they are considering investing? Will the media seek to determine what prescription drugs celebrities are taking? Will direct marketers, or market researchers, have access to information about patients' prescription and nonprescription drug use, either from medical records or from pharmacies? To what extent might employers demand medical information? (See footnote 23) The Report of the Work Group on Computerization of Patient Records recognizes that:

> as capability for storage and analysis of personal records increases and the cost of collection decreases, the demand for such information by providers, payers, policymakers, and researchers will likely multiply. There may be pressure to collect more data than is strictly necessary for a given purpose–collected data may then be maintained in a large database where it may be vulnerable to misuse. (See footnote 24)

Others are concerned that extensive access to medical records and health care information may pose a threat to privacy, and that safeguards against unauthorized access are meaningless if authorized access is so broad. (See footnote 25) Still others point out that, once any kind of information is compiled for whatever legitimate goal, the impulse to access that information for another well-meaning purpose is strong. (See footnote 26) The technology of computerization and security makes it possible to monitor information flow in computer systems, and enables society to enforce clear value choices as to whom information should properly be made available. (See footnote 27) Some suggest that this presents an opportunity for a reassessment of the question of authorized access, who should have it, and under what circumstances. (See footnote 28) Resolution of these issues would allow software developers to design systems in which access and security provisions for appropriate secondary users become a part of the computer system. (See footnote 29)

2.4 ISSUES RAISED BY COMPUTERIZATION

In view of the report by the Krever Commission, discussed in box 2-B, and from anecdotes of the kind presented in box 2-A it is clear that it is easy to gain access to, copy, remove, and destroy paper patient records. However, computers create new and more clearly defined problems about confidentiality and privacy than exist in paper record systems, and also bring longstanding confidentiality and privacy issues into sharper focus. Computerization of data with appropriate security measures can address the problem of confidentiality in sensitive medical information. Security alone, however, cannot solve the problem of patient privacy. The maintenance of medical information on computers also worsens some problems and raises new and complex issues not confronted in a paper environment. Legislation to address concerns about privacy in this information must apply to paper records, to computerized ones, and to the period of transition between paper and computers.

As discussed earlier, electronic storage and management of medical information is believed to provide certain advantages in the delivery of health care:

- It could allow for greater mobility of patient treatment within the health care system, which could foster competition for patients among health care providers.
- Use of an electronic system could potentially increase the speed with which patient medical histories could be accessed, thereby speeding treatment, particularly in medical emergencies.
- It has been suggested that computer records are better protected through computer security measures, thus eliminating the potential for abuse presented by paper records.
- Some suggest that the computer record allows greater control by part of record-keepers over patient information so that information based on need-to-know can be released to third-party payers, utilization review boards and other appropriate parties, replacing the current practice of releasing the entire patient record to process one insurance claim. (See footnote 30)

However, computerization of health care information raises other concerns:

- Computer technology makes the creation of new databases and data entry easy, so that databases can be created and maintained read ily. This could result in a proliferation of data and information that is easily searchable.
- Computerization allows for storage of large amounts of data in a very small physical medium. An intruder into a database can retrieve large amounts of data (most likely far more than could be stolen on voluminous paper records) once access is gained.
- Computers provide for the possibility of "invisible theft"–stealing data without taking anything physical– so that patients and providers remain unaware that the data has been stolen, altered, or abused.

- Computers allow for the possibility of "invisible" modification, deletion, or addition of data. (See footnote 31)
- Computers create the potential for the easy linking of data that were not intended to be collated. (See footnote 32)
- Computers allow a large number of people to handle or access data; the potential vulnerability of the data to large-scale intrusion is significantly increased in a computerized environment. (See footnote 33)

In sum, computer systems create easy opportunities to compile and maintain large amounts of information and to use it in ways that were never intended by the person who provided it. (See footnote 34) The compilation of data and the ease with which the information contained in the databank can be transferred by computer make access to that information easier and more attractive to a wider group of people. (See footnote 35)

2.5 RIGHT TO PRIVACY IN HEALTH CARE INFORMATION

Privacy in health care information has tradition ally been protected through ethical codes and through State and Federal laws. In addition, the Supreme Court has found sources for a right to privacy in health care information in the Constitution (see box 2-E).

2.5.1 Ethical Origins

The historical origin of the health care provider's obligation to protect the confidentiality of patient information is traced to the Oath of Hippocrates, written between the Sixth Century B.C.E. and the First Century A.C.E. which states:

> What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself. . .

Confidentiality requirements for physicians were formulated differently in later ethical codes. Thomas Percival's code of medical ethics, published in 1803 included the language:

> Secrecy and delicacy, when required by peculiar circumstances, should be strictly observed. And the familiar and confidential intercourse, to which the faculty are admitted in their professional visits, should be used with discretion and with the most scrupulous regard to fidelity and honor.

The first code of Ethics of the American Medical Association, adopted in 1847, was based on Percival's Code. The Code's provisions on confidentiality repeated the language of Percival's Code without substantive change, and continued:

> The obligation of secrecy extends beyond the period of professional services–none of the privacies of personal and domestic life, not infirmity of disposition or flaw of character observed during professional attendance, should ever be divulged by [the physician] except when he is imperatively required to do so. The force and necessity of this obligation are indeed so great, that professional men have, under certain circumstances, been protected in their observance of secrecy by courts of justice.

The American Medical Association's ("AMA") Principles of Medical Ethics expand on the ethical confidentiality obligation, requiring physicians to "safeguard patient confidences within the constraints of the law." (See footnote 36) In addition, the AMA's Council on Ethical and Judicial Affairs issued guidelines for maintaining confidentiality of health information in the Electronic Data Interchange environment. These guidelines require that the physician and patient consent to release of patient-identifiable clinical and administrative data to any entity outside the medical care environment. The guidelines also state that the release of confidential health information should be confined to the specific purpose for the release, and the recipient of the information should be advised that further disclosure is not authorized.

The AMA's Code of Ethics evolved from 1847 until the version drafted in 1980, in which confidentiality is covered in the fourth of eight principles.

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

The obligation to preserve patient confidentiality remained in the 1980 code, without any specific guidelines about how to respond to requests for information from researchers, police, Federal agencies, or other potential users of information. Nor is the term "patient confidence" defined.

Recent policy statements of the AMA more clearly detail the responsibilities of physicians to protect patient rights to confidentiality and the medical records. In the Code of Medical Ethics (Current Opinions, 1992), the AMA expresses its belief that the information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree.

> The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services. The patient should be able to make this disclosure with the knowledge that the physician will respect the confidential nature of the communication. The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.

The document sets forth particular instances when the obligation to safeguard patient confidences is subject to exceptions for legal and ethical reasons:

> Where a patient threatens to inflict serious bodily harm to another person and there is a reasonable probability that the patient may carry out the threat, the physician should take reasonable precautions for the protection of the intended victim, including notification of law enforcement authorities. Also, communicable diseases, gun shot and knife wounds, should be reported as required by applicable statutes or ordinances. (See footnote 37)

Other providers and organizations maintaining records have established standards to protect the confidentiality of health information. The American Hospital Association's Patient's Bill of Rights states that the patient has the right:

> . . . to expect that all communications and records pertaining to his/her care will be treated as confidential by the hospital and any other parties entitled to review certain information in these records.

2.6 FEDERAL LAW PROTECTING PRIVACY IN MEDICAL RECORDS

The Federal Privacy Act: The Federal Privacy Act of 1974, 5 U.S.C. Section 552a (1988) protects individuals from nonconsensual government disclosure of confidential information. The Act prohibits Federal agencies, including Federal hospitals, from disclosing information contained in a system of records (see footnote 38) to any person or agency "without prior written consent of the individual to whom the record pertains" unless the disclosure or further use is "consistent with" the purpose for which the information was collected. (See footnote 39) The purpose of the Privacy Act is "to provide certain safeguards for an individual against an invasion of privacy." (See footnote 40) The Act contains major requirements concerning collection, maintenance and dissemination of personal information. Agencies must:

1. Permit an individual the right to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies.

2. Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent.

3. Provide a procedure by which an individual may request the correction or amendment of information pertaining to them.

4. Be subject to civil suit for damages that occur as a result of willful or intentional action that violates any individual rights under the Act. The Privacy Act permits exemptions from the requirements for re cords provided in the Act only in those cases where there is an important public policy need for such exemption as determined by statutory authority (e.g., law enforcement).

Thus, the Privacy Act requires Federal agencies to collect, maintain, use, or disseminate any record of identifiable personal information in a manner that ensures that such actions are for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent its misuse. Hospitals operated by the Federal Government are bound by the Privacy Act's requirements with respect to the disclosure of the medical records of their patients. Also, medical records maintained in a records system operated pursuant to a contract with a Federal agency are subject to the provisions of the Privacy Act. For example, hospitals that maintain registers of cancer patients pursuant to a Federal contract or to federally funded health maintenance organizations are subject to the Privacy Act. (See footnote 41)

Alcohol and Drug Abuse Laws: Two Federal statutes prescribe special confidentiality rules for the records of patients who seek drug or alcohol treatment at federally funded facilities. (See footnote 42) These statutes and their implementing regulations apply strict confidentiality rules to oral and written communications of "records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any" educational, rehabilitative, research, training, or treatment program relating to drug or alcohol abuse. (See footnote 43) The regulations define a patient's record as "any information, whether or not relating to a patient, received or acquired by a federally assisted alcohol or drug program." (See footnote 44) In essence, these restrictions provide for a higher level of confidentiality and allow limited exceptions for release of patient information. These exceptions, however, allow disclosure with the prior written consent of the patient (if the consent meets certain requirements prescribed by regulation). (See footnote 45) These regulations have full force and effect of Federal law, so that they supersede State laws on confidentiality.

Section 1106 of the Social Security Act: This statute prohibits disclosure of any file, record, or other information obtained by the officers or employees of the Department of Health and Human Services except as prescribed by regulation. This prohibition also applies to officers and employees of any agency, organization, or institution that contracts with the Secretary (intermediaries and carriers) during the course of carrying out the contract. The regulations that implement section 1106, 42 C.F.R. secs. 401.101-401.152, supplement and are consistent with the regulations that implement the Federal Freedom of Information Act. (See footnote 46)

2.7 SOURCES OF THE CONFIDENTIALITY OBLIGATION–STATE COMMON LAW

Defamation. Defamation is the false written or oral communication to someone other than the defamed of matters that concern a living person and tend to injure that person's reputation. (See footnote 47) Medical records may contain information that is inaccurate and that, if published, would tend to affect a person's reputation in the community adversely. Thus, conceivably, disclosure by a hospital to an unauthorized person would result in an action for defamation. A qualified privilege may exist where information is transmitted to a third party with a proper motive or purpose and with the exercise of reasonable care that the information was true. (See footnote 48)

Breach of Contract. Courts have, of late, 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. As discussed above, the ethical standards of the AMA prohibit physicians in most situations from revealing a confidence entrusted to them by a patient during treatment. Further, the Medical Practice Acts of many States require physicians to maintain the confidentiality of their patients' medical information, and the AMA has published standards of hospital conduct that require hospitals to protect their patients' privacy. (See footnote 49) Some courts now appear willing to enforce these standards as part of the contractual relationship between physicians and their patients.

In Hammonds v. Aetna Casualty and Surety Co., (see footnote 50) the court held that a physician breached an implied condition of his physician-patient contract when he disclosed medical information to a hospital's insurer without the patient's consent. The court emphasized the rights of patients to rely on the ethical standards of confidentiality as on an express warranty. Similarly, in Doe v. Roe (see footnote 51) the court found both breach of contractual covenant to keep statements in confidence and a tortuous invasion of privacy when defendant published a book including an extensive transcript of statements made by the plaintiff patient during treatment.

2.8 SOURCES OF CONFIDENTIALITY OBLIGATION–STATE STATUTES

There is tremendous variation in the number and quality of State laws on medical confidential ity. While it may be difficult to generalize about the adequacy of State medical confidentiality laws, a report of the Committee on Government Operations of the House of Representatives concluded in 1980 that "most States do not have well defined, modern laws on the confidentiality of medical records." (See footnote 52) A survey of State statutes governing privacy in medical records published by Robert Ellis Smith emphasizes this point. (See footnote 53)

These statutes, however, do not address the flow of medical information to secondary users outside the treatment process, who are deemed to legitimately have access to the information. They do not address the responsibilities of third-party payers in handling this information, nor do they impose rules about the use of medical information by secondary users of that data: parties that use medical records for nonmedical purposes. This patchwork of law addressing the question of privacy in personal medical data is inadequate to guide the health care industry in carrying out its obligations in a computerized environment.

Furthermore, States are not consistent in their acknowledgment of the computerized medical record, and do not confront the problems presented by computerization. Some States continue to require that patient records be maintained in writing. Moreover, State law does not address the growing segment of the information industry that seeks to compile (whether with or without patient names or identifiers) medical information about patients for sale to interested corporations. (See footnote 54) As the WEDI Report to the U.S. Department of Health and Human Services states:

Myriad laws and regulations require providers to maintain health information in a confidential manner. . . [C]onfidentiality has historically been addressed at the state level, with each state crafting its own unique approach. The state rules are superimposed on a federal regulatory frame work. The result: a morass of erratic law, both statutory and judicial, defining the confidentiality of health information. (See footnote 55)

2.9 INADEQUACY OF EXISTING PROTECTION SCHEME AND THE NEED FOR FEDERAL LEGISLATION

Legal and ethical principles currently available to guide the health care industry with respect to obligations to protect the confidentiality of patient information are inadequate to address privacy issues in a computerized environment that allows for intra- and interstate exchange of information for research, insurance and patient care purposes. Lack of legislation in this area will leave the health care industry with little sense as to their responsibilities for maintaining confidentiality. It also allows for a proliferation of private sector computer databases and data exchanges without regulation, statutory guidance, or recourse for persons wronged by abuse of data.

The scheme, as it exists, does not adequately take into account the tremendous outward flow of information generated in the health care relationship today (see box 2-F and figure 2-1). This problem has always existed, but was not as serious because medical records were only occasionally used outside the medical treatment process. The expanded use of medical records for nontreatment purposes exacerbates the short comings of existing legal schemes to protect privacy in patient information. The law must address the increase in the flow of data outward from the medical care relationship by both addressing the question of appropriate access to data and providing redress to those that have been wronged by privacy violations. Lack of such guidelines, and failure to make them enforceable, could affect the quality and integrity of the medical record itself.

Further, the reservation of regulation of these matters to the States does not address the growing reality that this information will increasingly be transferred or accessed across State lines. As a result, health care providers, third party-payers, and secondary users of medical information will remain uncertain as to the law under which they are operating. The WEDI Report echoes this concern:

The regulatory framework governing providers' disclosure of patient-identifiable health information is flawed. It dictates different disclosure rules for different types of providers. These rules may conflict within a given state and among different states. The great variance in disclosure rules creates inconsistent standards for providers and offers inconsistent protection to patients. Some states offer little protection for health information, while others offer protection for the initial disclosure of information but ignore the problem of subsequent disclosures. (See footnote 56)

This lack of clarity could lead to increased litigation over medical confidentiality issues and the obligations of parties with access to the information.

Patient awareness that records are maintained on computers, absent the assurance of a clear law protecting the confidentiality of those records, could lead to deterioration of the traditionally confidential "physician-patient" relationship. (See footnote 57) Some contend that this breakdown could well lead to patients' withholding information critical to their care, thus jeopardizing their own health as well as denying the health care system (including physicians, nurses, hospitals, third-party payers, and researchers) information they may legitimately want and need, and that society has already deemed appropriate to give them. It could also place physicians in the difficult ethical position of deciding whether or not to enter sensitive information into the record at the patient's request (or maintaining a separate, noncomputer-based record), or the extreme of this situation, the development of a "black market" health care system that does not participate in the computerized exchange of patient information. (See footnote 58) Yet others argue that while patients do express concern about the privacy of their records in general, there is a body of medical literature that has found no significant patient concerns with the privacy of computerized medical records within private medical settings. (See footnote 59) While patient concerns may be lessened when their medical records are stored in the computers of their personal physicians, patients may be more concerned with records stored in the large, national databases that are proposed as a part of recent health care initiatives. (See footnote 60)

2.10 FOOTNOTES

1 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. 24. This is a publication of the Committee on Improving the Patient Record, Division of Health Care Services Institute.

2 Ibid.

3 The Institute of Medicine study cites a 1991 report of the U.S. General Accounting Office (GAO) on automated medical records. That report identified three ways that such records could benefit health care. GAO stated that automated records could improve delivery of health care by providing medical personnel with better data access, faster data retrieval, higher quality data, and more versatility in data display. Automated records could also support decision making and quality assurance activities and provide clinical reminders to assist in patient care. According to GAO, automated records could enhance outcomes research by electronically capturing clinical information for evaluation and could increase hospital efficiency by reducing costs and improving productivity.

4 Membership of CPRI includes representatives of health profession organizations such as the American Medical Association, the American Hospital Association, the American Medical Informatics Association, American Nurses Association, the American Health Information Management Association, the American Association for Medical Transcription, computer and telecommunications companies, and health maintenance organizations.

5 U.S. Department of Health and Human Services, Workgroup for Electronic Data Interchange, Report to the Secretary, July 1992, Executive Summary, p. iii.

6 Institute of Medicine, op. cit., footnote 1, p. 103.

7 U.S. Department of Health and Human Services, Work Group on Computerization of Patient Records, Report to the Secretary, "Toward a National Health Information Infrastructure," April 1993.

8 Harris-Equifax Consumer Privacy Survey 1992, conducted for Equifax by Louis Harris and Associates in association with Alan F. Westin, Columbia University. See also, Joel Reidenberg, Associate Professor of Law, Fordham University School of Law, testimony before the House Committee on Energy and Commerce, Subcommittee on Telecommunications and Finance, Oversight Hearings on Issues Related to the Integrity of Telecommunications Networks and Transmissions, Apr. 29, 1993.

9 Charles Piller, "Privacy in Peril," Macworld Special Report on Electronic Privacy: Workplace and Consumer Privacy Under Seige, July 1993, p. 8.

10 David Flaherty, "Ensuring Privacy and Data Protection in Health and Medical Care," prepublication draft, Apr. 5, 1993, p. 8 (citing Michael Isikoff, "Theft of U.S. Data Seen as Growing Threat to Privacy," The Washington Post, Dec. 28, 1991, and "Dealing Federal Information to Private Resellers," Privacy Journal, vol. 17, No. 3, January 1992, pp. 1, 4).

11 Charles Piller, op. cit., footnote 9, pp. 11-12.

12 Madison Powers, Joseph and Rose Kennedy Institute of Ethics, Georgetown University, personal communication, May 1993.

13 Alan Westin, Computers, Health Records, and Citizen Rights (Washington, DC: U.S. Government Printing Office, 1976) p. 9.

14 S. Rept. 101-116, on The Americans With Disabilities Act of 1989, 42 U.S.C. Sec 12101, P.L. 101-336, sets forth in detail the kinds and extent of discrimination that can result on the basis of a medical condition. The report cites specifically the testimony of a woman who was fired from the job she held for a number of years because the employer found out that her son, who had become ill with AIDS, had moved into her house so she could care for him. It also cited testimony of former cancer patients and persons with epilepsy, among others, who had been subjected to similar types of discrimination. Among the report's conclusions is that "[h]istorically, individuals with disabilities have been isolated and subjected to discrimination and such isolation and discrimination is still pervasive in our society." While the Americans With Disabilities Act can address the problem legally, it does not solve the problem of social stigma and social ostracism that can result when a person's medical condition becomes known.

15 For example, is information on chronic health conditions, when used to determine whether or not to employ specific individuals, sensitive? Different persons will also vary in their perceptions of what is sensitive, and thus what constitutes an invasion of privacy may vary from person to person. Joan Turek-Brezina, Chair, Department of Health and Human Services Task Force on the Privacy of Private Sector Health Records, personal communication, April 1993. Some commentators suggest that medical information is so sensitive that it deserves a special standard for protection under the law, one higher than that provided for say, financial or consumer information. Jeff Neuberger, Brown, Raysman and Millstein, New York, NY, personal communication, April 1993.

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

17 American Medical Association, Code of Medical Ethics, Current Opinions, Prepared by the Council on Ethical and Judicial Affairs, 1992, sec. 5.07.

18 For further discussion of the Medical Information Bureau, its purpose and activities, see further discussion in box 2-E.

19 Commentators note that this practice contributes to inadequate healthcare coverage for many Americans. Margaret Amatayakul, Associate Executive Director, Computer-based Patient Record Institute, Inc., personal communication, April 1993.

20 Institute of Medicine, op. cit., footnote 1, p. 21.

21 HCFA Data Compendium, Health Care Financing Administration, Fiscal Year 1992, U.S. Department of Health and Human Services, Bureau of Data Management and Strategy, Office of Statistics and Data Management, p. 28.

22 Federal Privacy of Medical Information Act, Report 96-832 Part 1, Mar. 19, 1980, p. 30.

23 Gerry D. Lore, Associate Vice President and Director, Government Affairs, Hoffmann-LaRoche Inc., personal communication, April 1993.

24 Report of the Work Group on Computerization of Patient Records, op. cit., footnote 7, p. 14.

25 If individuals perceive that personal medical information is at risk of broad authorized access, individuals may forego medical treatment. Gerry D. Lore, op. cit., footnote 23.

26 OTA workshop, July 1992. One example of this phenomenon is the use of taxpayer information to track parents whose child support payments are delinquent.

27 Alan Westin, Professor of Public Law and Government, Columbia University, personal communication, February 1993.

28 Gerry D. Lore, op. cit., footnote 23.

29 It is well established that computer security systems are best integrated into systems as the software is developed. Kevin McCurley, Senior Member of Technical Staff, Algorithms and Discrete Mathematics Department, Sandia National Laboratories, personal communication, November 1992.

30 OTA Workshop, July 31, 1992. Insurers' requests may be specific while the response to the request may be much broader than the request would require. Steven Brooks, Manager, Medical Information Management, Aetna Health Plans, personal communication, April 1993.

31 Ontario Commission of Inquiry Into the Confidentiality of Health Information, "Report of the Commission," 1980, vol. II, pp. 160-166.

32 This linkage of data is further facilitated by identification of data by Social Security Number, if it is used.

33 Steven Brooks, op. cit., footnote 30.

34 Ontario Commission of Inquiry Into the Confidentiality of Health Information, op. cit., footnote 31.

35 OTA Workshop, July 31, 1992. Some argue that once data is compiled for a particular purpose, the desire to use it for some other "laudable goal" becomes irresistable. Janlori Goldman, Director, Privacy and Technology Project, American Civil Liberties Union, personal communication, July 1992.

36 AMA Principles of Medical Ethics, Principle IV.

37 Code of Medical Ethics, Current Opinions, The American Medical Association, 1992. The AMA addresses these concerns again in its Policy Compendium: Current Policies of the American Medical Association, House of Delegates through the 1991 Interim Meeting. In its Policy Compendium of 1991 the AMA Council on Long Range Planning and Development discusses "Fundamental Elements of the Patient-Physician Relationship." Among these are the patient's right to confidentiality ("The physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest."), and the patient's right to obtain copies or summaries of their medical records. (Section 140.975, Fundamental Elements of the

Patient-Physician Relationship, subsections [4] and [1], respectively.) Special sections of the document state specifically the AMA's support for continued efforts to ensure the confidentiality of information on medical records, and encourages consideration of AMA drafted model state legislation, as well as its support for appropriate efforts to protect the confidentiality and privacy of information contained in electronic medical records.(Section 315.993, 998). It also addresses concerns about confidentiality of information requested by third party payors and utilization review groups. (Section 320.979 and 320.986).

38 Section 552a(a)(4) of the Privacy Act defines, for purposes of the Act, the term "record" as "any item, collection or grouping of information about an individual that is maintained by an agency, including but not limited to his education, financial transactions, medical history and criminal or employment history and that contains his name, or the identifying number, symbol or other identifying particular assigned to the individual such as finger or voice print or a photograph."

The Act defines the term "system of records" as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other indentifying particular assigned to the individual."

39 Ibid. Section 552a(b). Agencies have expanded upon the notion of "consistent with" to justify further uses of personally identifiable information.

40 Public Law 93-579, sec. 2(b).

41 Medical Records and the Law, William H. Roach, Jr., Susan N. Chernoff, Carole Lange Esley, eds., (Rockville, MD: Aspen Systems Corp., 1985) p. 78.

42 42 U.S.C. secs. 290dd-3, 290ee-3 (1988).

43 42 C.F.R. secs. 2.1 et seq., (1990).

44 42 C.F.R. sec. 2.12(e)(4), (1990).

45 See 42 C.F.R. sec. 2.31 (1990).

46 5 U.S.C. sec. 5552 (1988).

47 W. Prosser, Law of Torts secs. 111, 116 (1984).

48 In Gilson v. Knickerbocker Hospital 280 App. Div. 690, 116 N.Y.S. 2d 745 (1952), plaintiff sued the hospital for libel, claiming that, by complying with a subpoena, the hospital had maliciously allowed the publication of false and defamatory matter contained in the medical record. The record contained an observation that the plaintiff was under the influence of alcohol. The court granted the hospital's motion for summary judgment, stating that the defendant's act was absolutely privileged in that it was acting pursuant to lawful judicial process.

49 American Medical Association, A Patient's Bill of Rights (1972).

50 237 F.Supp. 96 (N.D. Ohio 1965) and 243 F. Supp. 793 (N.D. Ohio 1965). Applying Ohio law, the court held that a physician breached an implied condition of his physician-patient contract when he disclosed medical information to a hospital's insurer without patient's consent.

51 193 Misc. 2d 201, 400 N.Y.S. 2d 68 (Sup. Ct. 1977).

52 H.R. Rep. No. 832 pt. I, 96th Cong., 2d Sess. 30-31 (1980).

53 Compilation of State and Federal Privacy Laws, published by the Privacy Journal, Providence Rhode Island, 1992. For another review of the State law governing this issue see Medical Records and the Law, op. cit., footnote 4 app. B, State-by-State Analysis of Medical Records Statutes and Regulations.

54 Two such enterprises, PCN Inc. and PCS Health Services, Inc., are discussed in box 2-E.

55 Workgroup for Electronic Data Interchange, op. cit., footnote 5, app. 4, p. 5.

56 Ibid., p. 17.

57 OTA Workshop, July 31, 1992.

58 Ibid., Robert M. Gellman, "Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy," North Carolina Law Review, vol. 62, 1984.

59 See, A. Potter, "Computers in General Practice: The Patient's Voice," Journal of the Royal College of General Practice, vol. 31, 1981, pp. 83 to 85; M. Pringle, S. Robins, and G. Brown, "Computers in the Surgery: The Patient's View." British Medical Journal, 1984, vol. 288, pp. 289-291. G. Brownbridge, G. Hermark, and T. Wall, "Patient reactions to doctors' computer use in general practice consultations." Social Science Medicine, 1985, vol. 20, pp. 47-52. J. Rethans, P. Hoppener, G. Wolfs, J. Diederiks, "Do personal computers make doctors less personal?" British Medical Journal, 1988, vol. 296, pp. 1446-1448. Because medical computerization is further advanced in England than in the United States, these studies are predominantly surveys of patient opinion within the British working class. Similar findings have been reported in American work. See, J. Legler, R. Oates. "Patient Reactions to Physician Use of Computers During Clinical Encounters." Prepublication draft.

60 James D. Legler, M.D. Assistant Professor, Department of Family Practice, University of Texas, Health Science Center at San Antonio, personal communication, April 1993.

3 SYSTEMS FOR COMPUTERIZED HEALTH CARE INFORMATION

Implementation of a system for computerized medical information involves technological and nontechnological elements. Among the technological aspects of such a system are the online or off-line approaches to maintaining and processing information, computer security systems, and standards for computerization of medical information and the content of the medical record. From an administrative and policy standpoint, computerization of health care information requires foolproof identification of patients and patient information, policies to clarify questions of ownership and access to patient records, and practices for obtaining informed consent from patients for release and use of their personal data.

3.1 THE TECHNOLOGY OF COMPUTERIZED HEALTH CARE INFORMATION

Early research into computerization of medical information focused on administrative record keeping, laboratory management, and electrocardiographic analysis. In addition to these uses, one of the goals of this research has been the creation of an electronic, computer-based patient record. Computer systems for health care information records consist of four essential elements:

Hardware , including a central processing unit, mass storage devices, communication channels and lines, and remotely located devices (e.g., terminals or microcomputers with or without local area networks) serving as human/computer interfaces;

Software , including operating systems, database management systems, communication and application programs;

Data , including databases containing patient information; and

Personnel , to act as originators and/or users of the data; health care professionals, paramedical personnel, clerical staff, administrative personnel, and computer staff. (See footnote 1)

These elements have traditionally been contained within each medical institution, and each department within the medical facility has been linked to provide access to information by health care practitioners and administrators working at the facility. Privacy and security concerns have been addressed by the individual institution. Recently, however, faced with rising costs and increasing demands for more cost-effective delivery of services, the medical community is considering a system that links computers among institutions. Such an approach, an online system, would tie together computer systems in hospitals, private practitioners' offices, health maintenance organizations, health libraries and research resources, and third-party payers. Information about the individual patient could be transferred among these facilities, with the intent of eliminating paperwork and lowering administrative costs, while raising the level of patient care. (See footnote 2) Linkage of these computer systems would expand access and broaden security and privacy concerns.

A smart card system has also been considered as the primary means of storing and maintaining the patient record, or for use as an access control device to assure confidentiality in an online system, or some combination of the two. (See footnote 3)

Smart card systems for health care have been implemented extensively in France. Other European countries have pilot projects to test this technology for maintenance of health care data. Smart cards can be used in two ways: for storage of medical information, and for enhancing security of online computer systems. Smart cards are considered by some as a way of giving the patient maximum control over the confidentiality of his or her health care information. However, depending on how smart cards are used, they too raise concerns about privacy.

Whatever the technology employed to maintain medical information, decisions about privacy in data involve balancing the individual's right to privacy against the cost of security, and the impediment that security measures impose on the accessibility of data. Individual rights must also be balanced against public interests in informa tion such as those for medical research. (See footnote 4) Technology controls improper access from outside the system, but the greater concern for abuse is improper actions by persons authorized to access the computer system from within an institution. (See footnote 5) No system can be made totally secure through technology.

3.1.1 Online Systems

The Institute of Medicine (IOM) report discusses the potential for linking data in terms of "connectivity"– a term denoting the potential to establish links or to interact with any source or database that may improve the care of the patient. The report identifies three interfaces important for such interactions: 1) the interface between the record and other repositories or potential repositories of information that may be useful in providing patient care, 2) the interface between the record systems of different provider institutions, and 3) the interface between the record and a practitioner.

The ability to link these kinds of data depends on new network technologies that are built on communications, computing, information and human resource capabilities, and integration of computing and communications technologies to enable transmission of text, images, audio and video. The information infrastructure enabling these developments include communications net works, computers, information and the people who use these resources and create information.

Communications networks are interconnected and interoperable public and private communications networks ("public" networks refer to those networks, such as the public switched telephone network, that are open to use by anyone (common carriers); "private" networks refer to those that are limited to use by a specific group of people meeting certain criteria, such as corporate networks or "value added networks") providing services ranging from high to low speed, allowing a range of uses anytime, anywhere. They also involve agreed-upon technical standards for piecing together the network and having all the elements work together; the capacity to transmit information at both low and high speeds, in a variety of data formats, including image, voice, and video; and multiple mechanisms to support the electronic transfer of funds in exchange for services received.

Computers include specialized computers resident on the communications networks to provide intelligent switching and enhanced network services, personal computers and workstations, including machines that respond to handwritten or spoken commands and portable wireless devices that are easy to use and that can be easily accessed by users, and distributed computer applications that are widely accessible over the network.

Information includes public and private databases and digital libraries that store material in video, image, and audio formats, and information services and network directories that assist users in locating, synthesizing and updating information.

From a health care perspective, a high-performance computing network is believed to allow linkage of hospitals, doctors' offices, and community clinics through high-speed networks. Patient records, including medical and biological data, would be available to authorized health care professionals anytime, anywhere over these net works, allowing health care providers to access immediately, from any location, the most up-to-date patient data. This data would in the future include not only textual records but would also incorporate medical images (e.g., x-ray and magnetic resonance imaging) from clinical or laboratory tests. From an administrative standpoint, such a system could enable efficiency gains and cost savings. Most often cited is the projected savings in administrative costs involved in processing an estimated five million health care claims per day. It is believed that a network would allow improved management of and access to health care-related information and reduce costs for processing insurance claims through electronic payment and reimbursement. High-speed networks would also enable medical collaboration through use of interactive, multimedia telemedicine technologies over distances. (See footnote 6) The extensive linking of computers through high performance, interactive networks that enable instantaneous exchange of information challenges existing schemes for data protection, which place responsibility for confidentiality on each institution. Information will no longer be maintained, accessed, or even necessarily originate from a single institution, but will instead travel among a myriad of institutions, so that new systems for data protection must track the flow of the data itself.

3.2 SECURITY IN ONLINE SYSTEMS

In online systems, security is generally provided through the use of user identification names and passwords. User identification names can be defined in a variety of ways, including different combinations of segments of the patient's name and number sequences. Passwords are, theoretically, known only to the user and are periodically changed. More advanced technological solutions to the problem of access control include use of smart cards, or biometric control devices such as scanners that read finger-prints, retinas, or speech patterns. These devices provide heightened security, but at higher cost. (See footnote 7)

In addition to user identification names and passwords, systems may also be equipped with user-specific menus to control access to functions and thereby limit user access only to particular parts of the patient record that the user legitimately needs to carry out his or her job. Thus, an administrator may have the ability to view only accounting and demographic data and have no access to medical data. Indicators, or flags, can be used to define the level of interaction in a particular functional or domain area. For example, flags can control whether data can be accessed to be read or updated only; whether data can be corrected only on the same date of entry; whether data can be updated at a later date; and whether data can be validated or a process activated. Policy decisions may be made that certain kinds of information need not be accessible to all health care personnel. Thus, software can be implemented that suppresses and restricts access to certain categories of data. (See footnote 8)

Because a networked system allows access to data from a number of terminals, terminals may be left by the operator during a data entry session after the password has been entered and at a sensitive point in a query of the data entry process. This problem may be addressed by a mechanism for quick storage of information, and time-out features so that any idle terminal unused for input for a fixed period of time will automati cally revert to the password entry screen. (See footnote 9)

Some systems make use of audit trails, records of significant events (login, user authentication, and authorization, activities of specific users) that may be checked when something of a suspicious nature occurs. Audit trails can reveal irregular patterns of access and allow detection of improper behavior by legitimate or nonlegitimate users. (See footnote 10)

Equally as important in supplementing the technological measures taken to address the problem of maintaining a secure networked system are organizational education efforts, policies, and disciplinary "actions" to ensure the ethical behavior of persons inside the computer system who have authorized access to the information. In addition, organizational committees are often established to oversee and make decisions about compliance with regulations about data, legal concerns, and ethical considerations regarding the transfer and release of information.

3.2.1 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, (see footnote 11) memory, and an input/output interface. Smart cards can perform two major roles:

1. they can provide a medium for storing and carrying personal information; and
2. they can process information that enhances the security of many online computer systems, thus acting as a means for accessing information in a network of computers. (See footnote 12)

Definitions of what constitutes a smart card differ. Generally, a smart card encompasses off-line technology that is able to activate devices at the point of use. The traditional smart card, invented in 1974, is embedded with a microchip, which allows it to exchange information with a computer. The super smart card is battery- powered, contains a keyboard and display, and has a 64K EEPROM (Electrically Erasable Programmable Read Only Memory) (see footnote 13) reprogrammable memory chip and microprocessor for internal power. (See footnote 14)

The smart card reader/writer device is also a major component of the smart card system. The main purpose of the reader/writer device is to provide a means for passing information from the smart card to a larger computer and for writing information from the larger computer into the smart card. The reader/writer device provides power to the smart card and physically links the card's hardware interface to the larger computer. Since the smart card's microprocessor can control the actual flow of information into and out of the card's memories, the reader/writer device's role may be minimal. Some smart card systems incorporate reader/writer devices that perform calculations and other functions. It is generally the smart card itself that determines if and when data will be transferred into and out of the smart card's memories.

3.3 SMART CARDS AS A MEANS OF INFORMATION STORAGE. (See footnote 15)

The capacity of smart cards to store information has increased to 800 printed pages. In addition to this expansive memory, the smart card can ensure that the information stored in its memory is secure. The memory of a smart card can be divided into several zones, each with different levels of security and requirements for access, as required for a specific application. The smart card microprocessor and its associated operating system can keep track of which memory addresses belong to which zones and the conditions under which each zone can be accessed (see figures 3-1 and 3-2).

A confidential zone could be used to store an audit trail listing all transactions, or attempted transactions, made with the card. The confidential zone could have a password known only to the card issuer, who could examine the history of the card for evidence of misuses of the system. To prevent any attempts to modify the card's audit trail, the confidential zone could have a read-only access restriction, so that the system could write to the zone, but information could not be changed from the outside.

A usage zone could be used for storage of information that is specific to the smart card application and that requires periodic updates and modification. For example, the date of the card bearer's last access to the host computer or the amount of computer time used could be stored in the usage zone. Depending on the sensitivity of the data, a password could be required for this zone. The usage zone could have both read and write access protected by a password.

A public zone could hold nonsensitive information, such as the card issuer's name and address. The public zone could have read-only access, without a password.

Crucial secret information can be maintained in separate protected memory locations through the use of the smart card's memory zones. It may also be possible to produce a smart card that would ensure that the entire secret zone will be destroyed if any attempt is made to access the data in that zone; information located in that zone could be used only by the microprocessor itself. Information such as passwords, cryptographic keys, and other information which should never be readable outside of the smart card could be located here. The smart card's capacity for distinct memory zones also allows for the allocation of separate memory zones for individuals so that, for example, only the card bearer could access the usage zone, and only the card issuer could access the confidential zone.

Care providers would be equipped with a reader, microcomputer, and necessary software. Each provider would be given an accreditation card to gain access to the smart card of patients. This card defines the zones to which access is allowed. A Personal Identification Number (PIN) would also have to be entered before the smart card could be accessed (like those used by bank automatic teller machines and credit cards.)

3.4 SMART CARDS AS A MEANS OF ACCESS CONTROL

A smart card can be used as part of an access control system to protect sensitive data. Appendix A discusses generally the basic access control concepts of cryptography, user authentication, and device authentication. A smart card can be used to perform the encryption operations needed for authentication rather than a cryptographic device attached to (or inside of) a terminal (see figure 3-3). A smart card is intended to remain in the possession of its sole user, who is responsible for its protection, as opposed to a cryptographic device kept at the site of the terminal, which may be vulnerable to tampering. The cryptographic operations performed by a smart card are believed to possess the potential to improve security.

In addition, the smart card is capable of encrypting short strings of data used in authentication procedures. Several encryption algorithms are currently available in smart cards and implementations of the Data Encryption Standard have been developed for smart cards.

3.5 THE SMART CARD AS A CARRIER OF MEDICAL DATA

The concept of a patient card and the portable medical record was originally born in the 1970s, but it took several years, until the mid 1980s, to implement the operation. (See footnote 16) The frequently used definition of a patient card is:

> . . . a plastic card of credit-card size upon which is printed legible information; it may also carry part or all of the patient's medical record in micro

or digital form. A card that carries only medical information is referred to as a "dedicated" patient card. Non-dedicated cards may carry insurance information, financial or credit data, educational data, etc., in combination with medical information. (See footnote 17)

Several countries are currently attempting to implement such a health care card (see box 3-A on the French Smart Card System for Health Care). In Australia, proposals for implementation of such a system provide that:

Patients will be able to elect to have a life-long health care record in electronic form, which will contain a summary of all relevant health care information from the date of birth until death. Included will be entries from general practitioners, specialists and consultants, radiologists, laboratories, nursing care, hospitals, physiotherapists, psychologists, occupational therapists, dental care etc. The total record will be carried by the patient on a "Health Card" the size of a plastic credit card. Copies will also be kept by the last doctor seen and by a "national back-up service" (a nongovernment organization) which will maintain a network of back-up centers throughout the country. This electronic record will have several levels of security restriction which will control who will have access to what part of each encounter. (See footnote 18)

In the Australian approach, the smart card will collate all patient information–administrative, hospital, and doctor related records.

Pilot projects have been implemented in France, Great Britain, (see footnote 19) Sweden, and Italy, which use the smart card in a different manner, storing limited kinds and amounts of information (see box 3-B). In the United States, card systems are proposed as one solution to the need to contain costs, streamline paperwork, and increase availability of health care services. (See footnote 20)

Smart card technology is often cited as a possible solution to the problem of privacy in computerized medical data. In lieu of a computerized, central database, or a linked network of information, smart cards would allow individual patients to maintain their own medical records, and would empower the patient with the ability to consent to any access to the data by authorization of access to the card. The smart card, as a patient-borne record, would represent a distributed database with the advantage that real-time access to information is available only with the informed consent of the patient (with the exception, probably, of emergency information). (See footnote 21) This is contrasted with the acknowledged risk of computer network penetration by the determined "hacker" who, if successful, could have access to thousands, even millions, of clinical records. The restriction of access to different kinds of data of different levels of sensitivity enabled through use of security codes arguably heightens the patient's personal control over the data. (See footnote 22)

However, critics of such a system cite short comings of the card's ability to protect patient privacy in medical information. Concerns have been raised about patient compliance with carrying the card. (See footnote 23) The proposed solution to such compliance problems is the creation of a back-up database containing the patient information, such as that proposed in the Australian plan (see discussion on pages 58-61). (See footnote 24) Such a database would, arguably, present many of the same problems as an online computerized system. Others have noted that while the smart card allows for control over the information while it is in the patient's possession, it is entirely possible that the patient will not know the nature of the information he or she is carrying. (See footnote 25) In addition, without further laws to the contrary, the carrier of the patient card could be completely dependent on the judgment of health care administrators to determine what information should be accessed by which health care provider, insurer or other third party. (See footnote 26) Concerns remain, also, about security of information at the host. (See footnote 27) Yet another concern is that patients will not want information about psychic and mental diseases, AIDS tests, abortions, venereal diseases, or genetic anomalies recorded on the card. As a result, there is concern about whether a smart card will contain a comprehensive medical record, or an abbreviated version of the record with its attendant limitations.

Some also contend that, while the patient data serves to document the process of patient care, it would be inappropriate to eliminate the hospital or office-based record of care because that record is also part of the process information of the health care provider. The proposed 1994 Accreditation Manual for Hospitals released by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) emphasizes the ever-increasing role of information in patient care processes as a way of measuring the quality and efficiency of health care delivery. Given this scenario, the card would more likely serve as the patient's personal copy, or would serve as an access control tool, but would not be the sole source of patient information. (See footnote 28) From the stand point of health care research, questions remain to what extent this system would hinder epidemiologists' efforts to examine the course of diseases through access to medical records. (See footnote 29) Still others indicate their 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. (See footnote 30)

3.6 THE UNIQUE PATIENT IDENTIFIER

Proposals for establishing a unique patient identifier have been the subject of much discussion. Proponents of the computerized patient record recommend the use of a unique patient identifier that is assigned to the patient at birth and remains permanently throughout the patient's lifetime. Theoretically, an identifier might allow appropriate information exchange between approved parties in the course of delivery of health care, and may ensure that accessed, entered or altered records correspond to the proper patient. The assignment of such a unique number might also prevent problems of fraud and forgery in the reimbursement process. It could also facilitate linkage of information for administrative, statistical, and research purposes.

A variety of systems for assigning such a number have been proposed, including some combination of parts of the Social Security number, segments of the patient's name, digits from the patient's date of birth, and the latitude and longitude coordinates of the patient's place of birth, or place of issuance of the number. (See footnote 31) The most often mentioned, and what is often argued to be the most expeditious solution, is the use of the Social Security number itself. (See footnote 32) While recognizing that problems exist in the assignment of the Social Security number while avoiding duplication and preventing forgery, many see this established system of a unique number for individuals to be the most efficient and cost effective way of dealing with the problem of the unique patient identifier. (See footnote 33)

In spite of the ease with which proponents believe that such a system might be put in place, and the advantages of such a system to facilitate record linkages that might permit improved delivery of health care and reimbursement, privacy advocates strongly criticize the proposal. (See footnote 34) Concerns about the proliferation of the use of the Social Security number for purposes unrelated to the administration of the Social Security system, and the power of the number to act as a key to uncovering and linking a vast amount of information held both by the government and private companies, (see footnote 35) have been voiced by many in a variety of contexts. Following passage of the Social Security Act in 1935, the narrowly drawn purpose of the Social Security number was to provide the Federal government with means of tracking earnings to determine the amount of social security taxes to credit to each worker's account. Over the years, however, the use of the number as a convenient means of identifying people has grown, so that the Social Security number has been used by government agencies and the private sector for other purposes. (See footnote 36)

As a result of this expanded use of the Social Security number, the number now facilitates the ability of large institutions to compare databases. It allows outsiders (including private detectives, computer hackers, or other strangers) to move from database to database, from credit bureau to insurance company to grocery store to publisher, to find out detailed marketing, financial, and medical information about an individual, so that a very detailed dossier on the individual can be created.

The Court of Appeals for the Fourth Circuit in Greidinger v. Davis (see footnote 37) noted that since the passage of the Privacy Act, an individual's concern about his Social Security number's confidentiality and misuse has become more compelling. The court discussed at some length the potential financial harm that can result from the number falling into the hands of an unscrupulous individual. At least as important, however, is the court's recognition that other illegal uses of the number include "unlocking the door to another's financial records, investment portfolios, school records, financial aid records, and medical records." (See footnote 38) While the adoption of any patient identification number should be carefully considered, use of the Social Security number as a unique patient identifier presents special privacy problems. Proposals to adopt the Social Security number, as opposed to some other unique patient identifier, should be closely scrutinized and alternative proposals considered as decisions are made about computerization of medical information.

Proponents of the use of such an identifier believe that, if appropriate safeguards are used, the integrity of the Social Security number can be maintained.

One suggestion is use of encryption to protect the number. (See footnote 39) Others argue that the solution to the problems presented by use of the Social Security number is not to devise an alternative system, but to create and enforce a policy that addresses the abuses to which the number may be subject. (See footnote 40)

The experience of Ontario, Canada with unique patient identifiers in delivering health care benefits is useful. (See footnote 41) All Canadian provinces have some type of health identification numbers. While some are permanent numbers, some change in the course of an individual's lifetime. Only the province of Prince Edward Island uses the Federal social insurance number, a number akin to the Social Security number in the United States, for health purposes.

Ontario introduced a system of unique, life time, 10-digit health numbers for all individuals in 1990. Privacy advocates in Ontario wanted to ensure the use of the new numbers for health- related purposes only, and to prevent their emergence as a universal unique identifier for residents of the province, as they believed had been the case with the social insurance number. (See footnote 42)

In response to these concerns, the Ontario legislature enacted the Health Cards and Numbers Control Act, which specifies that "no person shall require the production of another person's health card or collect or use another person's health number." The numbers can be used to provide health resources funded by the province and for "purposes related to health administration or planning or health research or epidemiologic studies." (See footnote 43)

3.7 STANDARDS FOR COMPUTERIZED MEDICAL INFORMATION

According to the IOM, in order to implement a computerized system for health care information, three kinds of standards must be developed: content, data-exchange, and vocabulary; patient data confidentiality; and data and system security. (See footnote 44) It is believed that these are necessary for transmitting complete or partial patient records, and that they are essential to the aggregation of information from many sources, either for longitudinal records for individual patients or for databases of secondary records to be used for research or epidemiologic purposes.

Content standards are to provide a description of the data elements that will be included in automated medical records, with the intent that uniform records will be produced no matter where or in what type of health care setting the patient is treated. Data-exchange standards are formats for uniform and predictable electronic transmis sion of data, establishing the order and sequence of data during transmission. Vocabulary standards establish common definitions for medical terms and determine how information will be represented in medical records. These standards are intended to lead to consistent descriptions of a patient's medical condition by all practitioners. (See footnote 45) Currently, the terms used to describe the same diagnosis and procedures sometimes vary. Data and system security standards are to ensure that patient data are protected from unauthorized or inadvertent disclosure, modification, or destruction. Health care providers, hospital administrators, researchers, policymakers, and insurers must agree on common levels of data protection before they can benefit from the widespread use of automated patient information. (See footnote 46)

Two kinds of standards must be developed for the content of computer patient records. One is a minimum data set that applies to all computer patient records; the second is content standards for specific kinds of computer patient records. Establishment of these standards would allow effective use of the patient record data by clinical and nonclinical users because record content would be consistent among various institutions and practitioners. There is also an effort to establish a specific meaning for data elements; data elements would be used to collect the same pieces of information in all record systems. Composite clinical data dictionaries would enable users to translate data from different systems to equivalent meanings.

Standardization of medical information in both content and format is believed to be of utmost importance in establishing a computerized system. (For discussion of standard development efforts, see box 3-C). The completeness of patients' records for subsequent users depends in part on agreement among users about uniform core data elements. Without such uniformity, what one patient-record user views as complete data may be considered incomplete by another. Data completeness implies that systems will accommodate the currently expected range and complexity of clinical data and that they will permit new data fields to be added and obsolete data to be identified. Standardization of medical information facilitates gathering, exchanging, and transmitting data. The combined effect of data compatibility provided by standards, coupled with networked computer information systems and the capacity to maintain enormous databases of personally identifiable information presents tremendous challenges to privacy.

While progress in development of standards in any of these categories is limited, efforts to develop security and confidentiality are in their early stages. (See footnote 47) Although there is general agree ment that this issue is critical, only one of the four standard setting organizations is addressing this topic. Work began in November 1991, and an early draft of the standards is being developed. The progress and decisions of standard setting organizations that are establishing minimum standards for confidentiality deserve careful examination, so that technology can best serve the protection of privacy.

The discussion of standardization of computer ized medical information includes the issue of patient record content, i.e., what information constitutes the patients' record. Standardization of the patient record content would allow health care practitioners, third-party payers, and second ary users of medical data to know what information would be available for patients under their care. Physicians and other medical personnel would know what personal identification, clinical and other data would be available for making medical decisions, even on a patient's first visit, or if an emergency situation arose. Third-party payers could process claims faster on the basis of standard and readily available medical, financial and administrative forms and information. Secondary users of medical data, such as researchers, utilization review committees, and public health workers, could anticipate the nature of the information available for research and policy decisions.

The nature and scope of the medical record highlights the question "what is medical information." (See footnote 48) The paper record is currently a repository for a wide array of information, including:

- the patient's name, address, age, and next of kin; names of parents;
- date and place of birth;
- marital status;
- religion;
- history of military service;
- Social Security number;
- name of insurer;
- complaints and diagnosis;
- medical, social and family history;
- previous and current treatments;
- inventory of the condition of each body system;
- medications taken now and in the past;
- use of alcohol and tobacco; diagnostic tests administered; and
- findings, reactions, and incidents. (See footnote 49)

Some argue that the record should include a tremendously broad range of information: demographic, environmental, clinical, financial, employment, family history, health history. Such an inclusive record would ensure the ready availability of information to health care workers and researchers. It would also, they argue, place all such information under the umbrella of whatever legal protections are afforded to medical records and information. (See footnote 50)

The response to this argument is that accumulation and storage of so much personal information would lead only to a greater chance for abuse as well as access to information by persons who do not really have a legitimate need to know. (See footnote 51) While plans exist to compile a "womb to tomb" longitudinal record, including all information from pre-birth to death, some advocate data destruction after an appropriate period of time. Medical information necessary to treat certain conditions can be reconstructed adequately to assure good quality medical care, they believe, so that massive amounts of highly personal and sensitive information need not be warehoused throughout the patient's lifetime. This approach, they believe, balances the medical "need-to- know" with the privacy interests of the patient. (See footnote 52) The decisions of organizations charged with establishing standards for patient record content deserve special scrutiny, as the medical record would be a significant subject for any legal protection of medical information.

3.8 INFORMED CONSENT TO DISCLOSURE OF INFORMATION

Because of the sensitive nature of health care information, physicians generally must obtain patient consent before disclosing patient records to third parties. (See footnote 53) The theory of informed consent to release of information originates in the concept of informed consent to medical treatment. Medical and research codes, as well as Federal regulations, have traditionally emphasized the elements of disclosure, voluntariness, comprehension, and competence to consent. (See footnote 54) For there to be informed consent to medical treatment, the act of consent must be genuinely voluntary, and there must be adequate disclosure of information to the patient about what is to be done. Patients must comprehend what they are being told about the procedure or treatment, and be competent to consent to the procedure. (See footnote 55)

On the basis of this model, if informed consent requires communication of information and comprehension by the patient of what he or she is being told, informed consent to disclosure of medical information is arguably possible only when patients are familiar with the data contained in their records, so that they understand what they are consenting to disclose. Because many patients are neither granted access to their medical records, nor apprised of which portions of the record are accessible to others, most patients are ill-equipped to make intelligent choices about authorizing disclosures. (See footnote 56)

The general rule is that the owner of the paper on which the medical record is maintained is the "owner" of the record. (See footnote 57) Some States have statutes that specify that health care facilities own the medical records in their custody. At the same time, physicians, even if not covered by statute, are considered the owners of the medical records generated by them in their private offices. How ever, ownership of a medical record is a limited right that is primarily custodial in nature. Licensing statutes and statutes governing contracts (e.g., health insurance contracts) place limits on the right of ownership in the record. Moreover, the information contained in the record is often characterized as the patient's property. (See footnote 58)

Early in the twentieth century, when sole practitioners dominated the medical profession, the typical medical record consisted of a ledger card noting the date of visit, the course of treatment, and the fees charged. The specialization of health care, the rise in clinical and outpatient care, and increased patient mobility have fostered greater interaction between the average individual and the health care system. In addition, the decline of the long-term, one-on-one physician-patient relationship made necessary more comprehensive medical records to provide continuity and communication within the medical community. The use of the medical record as a general source of information for decisions and control in nontreatment contexts also has proliferated. Access to the medical record has become vital to institutions which once had a marginal interest–but no legitimate need–for such personal information. Further, the medical record has assumed primary importance in Federal Government-mandated medical community audits of physician competency and performance and in insurance company assessments of an applicant's eligibility for health and life insurance. The medical record plays a role in insurance claims processing and in public and private efforts to detect medical fraud. Private employers, educational institutions, credit investigators, and law enforcement agencies also use personal medical information. Advances in information technology has matched this rising demand for medical records. It is this pervasiveness of disclosure and the potential for new demands for information that increases the patient's need to ensure the accuracy of the information contained in his or her medical record. With a right of access to the record, patients would have an opportunity to refuse consent to the release of information, challenge the accuracy of information, or request deletion of information irrelevant to the concerns of the party requesting disclosure. (See footnote 59)

In spite of the requests made of them to authorize disclosure of medical information for medical and nonmedical purposes, patients traditionally have been unable to inspect their own records, and laws governing patients' access to records are not universal or uniform. (See footnote 60) Because of the absence of limitations of these regulations, individuals are routinely denied access to their health information. This traditional lack of patient access to health records is based on the rationale that the physician, in accepting responsibility for the patient's health, needs broad discretion to withhold medical information that the physician deems harmful to the patient. (See footnote 61) The justification for this right on the part of the physician has been to protect patients from information that would be detrimental to their health. (See footnote 62) However, this approach to the patient record arguably conflicts with patient rights and autonomy. (See footnote 63)

Traditionally, the medical rationale for withhold ing information in the chart has been patient psychopathology or medical paternalism. Both rationales fail to address the issue of rights. Patients have rights because they are people. If we believe in individual freedom and the concept of self-determination, we must give all citizens the right to make their own decisions and to have access to information that is widely available to those making decisions about them. (See footnote 64)

While the majority of States grant individuals a legal right to see and copy their medical records by statute, regulation or judicial decision, (see footnote 65) laws regulating patient access to health records are not uniform or even universal. Federal regulations for substance abuse programs, (see footnote 66) "Confidentiality of Alcohol and Drug Abuse Patient Records," specifically permit individuals access to their own health records. Subpart B, Section 2.23 states: "These regulations do not prohibit a program from giving a patient access to his or her own records, including the opportunity to inspect and copy any records that the program maintains about the patient." Section 483.10(b)(2) of the new regulations for nursing facilities grants residents access to their records within 24 hours, and grants residents the right to obtain photocopies within two working days. Only 27 States have statutes requiring providers to make health records available to patients, and the majority of these statutes fall under hospital licensing acts. On the Federal level, the Privacy Act of 1974 provides for direct access to information under most circumstances. (See footnote 67)

Indeed, the Privacy Protection Study Commission, established by the Privacy Act, recommended that, "[u]pon request, an individual who is the subject of a medical record maintained by a medical care provider, or another responsible person designated by the individual, be allowed access to that medical record including an opportunity to see and copy it." (See footnote 68) The American Health Information Management Association (AHIMA) has taken the position that patients should have access to the information contained in their health records. The basis for establishment of this right is so that patients can:

1. be knowledgeable about the nature of their disease or health status and understand the treatment and prognosis;
2. be educated about their health status to enable them to participate actively in their treatment process and in wellness programs;
3. provide a history of their medical care to a new health care provider;
4. ensure the accuracy of documentation in the health record with regard to diagnoses, treatment(s), and their response to treatment(s);
5. verify that the documentation in the health record supports the provider's bill for services; and

6. be informed of the nature of the information being released to third parties such as insurers, when authorizing disclosure of their health information. (See footnote 69)

The AHIMA recommends limitations on access where patients are adjudicated incompetent, where the health care provider has determined information would be injurious to the patient or other persons,70 where State law specifically precludes access, and where minors are governed by legal constraints. (See footnote 71)

Patient access to their medical record is seen by some as part of a broader effort to expand and regularize regimes for ensuring informed consent from health care recipients to disclosure of medical information. In addition to patient understand ing of the contents of his or her medical record, some believe that individuals have a right to learn in considerable detail what will be done with their personal information at the time of initial contact with a health or medical organization or other care giver, even if many of the disclosures are mandatory. (See footnote 72) Some commentators suggest that patient consent forms for disclosure of information should be required to contain a check list detailing what information can be released, to whom it may be sent, for what purpose it may be used, and for what period of time. (See footnote 73)

Today, blanket consent forms are commonly used in health care. Patients are generally asked to sign such a form upon his or her entering the health care facility, and the form essentially states that the facility may release medical information concerning the patient to anyone it believes should have it or to certain named agencies or organizations. These agencies include insurance companies and the welfare department, and other cost and quality monitoring organizations. Usually no restriction is placed on the amount of information that may be released, the use to which these parties may put the information, or the length of time for which the consent form is valid. (See footnote 74)

Much of the debate about what constitutes informed consent centers on how much information is enough and how much is too much. Some argue that giving persons a long list of information about potential uses of their data would be an unwieldy process, since it would involve setting out all primary and secondary uses of the information. Such a requirement, they believe, would result in administrative confusion, if individuals exercise a right to reject or accept various uses. (See footnote 75) Yet others recommend at minimum "a policy decision not to honor statements of unrestricted scope." (See footnote 76) Resolution of questions of patient access and requirements for informed consent at the outset of establishment of computer system would enable software developers to incorporate appropriate software and access controls directly into new systems.

3.8.1 Alternatives to Informed Consent

Because informed consent must be voluntary, some argue that in the present health care system, and likely in future health care plans, the concept of informed consent is largely a myth and the mechanism of informed consent has no force. Medical information is most commonly required to provide health care reimbursers with sufficient information to process claims. Individuals for the most part are not in a position to forego such benefits, so that they really have no choice whether or not to consent to disclose their medical information. An alternative approach to informed consent is the notion that an individual gains access to medical benefits in exchange for reason able use of certain medical information by the system for prescribed purposes. Once that reason able use is determined, the system must then protect the use and the confidentiality of the information. Informed consent would then be required of individuals only when information about them were to be put to some extraordinary use.

3.9 FOOTNOTES

1 Gretchen Murphy, "System and Data Protection," Aspects of the Computer Based Patient Record, Marion J. Ball, Morris F. Collin, eds., (New York, NY: Springer-Verlog, 1992).

2 Wide linkage of computer systems has already been accomplished between financial institutions, allowing for, among other things, electronic funds transfer, and immediate, onsite verification of credit eligibility.

3 Suggestions have been made that the smart card might contain certain critical pieces of information, e.g., patient identification, special conditions or allergies, the name and phone number of the patient's primary physician, as well as act as an access control device.

4 Some commentators suggest that the fundamental question may be whether individual privacy in medical information is an absolute right, one not subject to a utilitarian balancing approach. That perspective suggests the more difficult issue, whether personal medical information should even be entered into a national computer system, regardless of the safeguards put in place. Gerry D. Lore, Associate Vice President and Director, Government Affairs, Hoffman LaRoche Inc., personal communication, April 1993.

5 Robert H. Courtney, "Considerations of Information Security for Large Scale Digital Libraries," contractor paper prepared for the Office of Technology Assessment, Mar. 27, 1993.

6 S. 4, Title VI - Information Infrastructure and Technology, introduced before the 103d Congress, sets forth applications of such a network for health care. These include networks for linking hospitals, clinics, doctors' offices, medical schools, medical libraries, and universities; software and visualization technology for visualizing the human anatomy and analyzing x-ray, CAT scan, PET scan imagery; virtual reality technology for simulating surgery and other medical procedures; collaborative technology to allow several health care providers in remote locations to provide real-time treatment to patients; database technology to provide health care providers with access to relevant medical information and literature; database technology for storing, accessing and transmitting patients' medical records while protecting the accuracy and privacy of the records. (Corresponding bill introduced before the House of Representatives, H.R. 1757.)

7 W. Ed. Hammond, "Security, Privacy and Confidentiality: A Perspective," Journal of Health Information Management Research, vol. 1, No. 2, fall/winter 1992, pp. 1-8.

8 Ibid. Harvard Community Health Plan, for example, restricts, among other things, certain kinds of narrative mental health data (notes, dictation, free text) in this manner.

9 Some organizations implement a policy whereby people who have not properly logged out of a system will be held responsible for improper access to data.

10 Audit trails only detect breaches in security "after the fact;" there must be a specific policy in place that such trails are regularly checked in order for them to be effective.

11 The microprocessor is the component which distinguishes a smart card from cards designed to simply store data. The microprocessor and its operating system enables the smart card to "make decisions" about where it will store data in its memories and under what circumstances it will transfer data through its input/output interface.

12 Smart cards and access technologies are only one part of an overall computer security program. For a discussion of computer security measures, see app. A.

13 EEPROM is a memory that can be electrically erased and reprogrammed via a reader/writer device at the user's facility.

14 Other cards not generally characterized as smart cards include magnetic stripe cards, which can store about 800 bits (100 bytes) of information. These are largely used as banking cards. High-density magnetic stripe cards are in the development stage. Using new magnetic materials, these cards would be able to carry one megabit or more. Memory cards involve the use of integrated circuits, but do not have a processor. Memory cards are often described as the immediate technological advance over magnetic stripe cards. The optical card or laser smart card is an optical memory card with laser-recorded and laser-read information that can be edited or updated and has a storage capacity of 800 printed pages. See, J.A. Reese, "Smart Cards: Microchip Technology Revolutionizes the Development of Bank Cards," Telecommunication Journal, vol. 59, No. 3, 1992, p. 134; and "Introduction to Smart Cards" Version 1.0, Reference GGA06U10, a publication of Gemplus Card International, 1990.

15 The sections on smart cards as a means of secure storage of information and as a means of access control are derived from 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," NIST Special Publication 500-157, September 1988, pp. 13-26.

16 Claudia Wild and Walter Peissl, "Patient Cards: An Assessment of a New Information Technology in Health Care," IT in Medicine, Project Appraisal, vol. 7, No. 2, June 1992, pp. 67-78.

17 Ibid.

18 Walker et al., Health Information Issues in General Practice in Australia, National Centre for Epidemiology and Population Health, Discussion paper No. 2, ANU, Canberra, 1991, cited by Simon Davies, Big Brother: Australia's Growing Web of Surveillance (Australia: Simon & Schuster, 1992), p. 54.

19 The Exmouth Project, conducted in Exeter, England, is discussed in 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. 78-79.

20 Major proposals before the 102d Congress concerning health care reform and involving the use of smart card technology included one by the Bush administration (originally issued as a White Paper in 1992, which discussed the issue of administrative costs and strategies to reduce them) introduced in both Houses as "The Medical and Insurance Information Reform Act of 1992" and three legislative proposals: S. 1227, "Health America: Affordable Health Care for All Americans Act" introduced by Senators Mitchell and Kennedy; H.R. 1300, "The Universal Health Care Act of 1991" introduced by Representative Russo; and H.R. 3205, "The Health Insurance Coverage and Cost Containment Act of 1991" introduced by Representative Rostenkowski. The 103d Congress introduced several new proposals, including H.R. 200, introduced by Congressman Stark, "Health Care Cost Containment & Reform Act of 1993"; H.R. 191, introduced by Congressman Gekas, "American Consumers Health Care Reform Act of 1993"; and S. 223 "Access to Affordable Health Care Act" introduced by Senator Cohen.

21 Some argue, however, that in and of themselves, smart cards could offer the technical capability to give the patient more control over medical information, but only if the medical data is completely and solely resident on the card. Sheri Alpert, "Medical Records, Privacy and Health Care Reform," prepublication draft, June 28, 1993. A version of this paper will appear in the November/December 1993 issue of the The Hastings Center Report.

22 Debate continues about who may examine which zones of the card, and who may make entries on the card.

23 The card is useless if lost, forgotten, or damaged. None of the current proposals for use of the cards suggests that the medical data reside solely on the card for that reason. In addition to concerns about compliance, there is also a potential for theft and fraudulent use of the cards.

24 Each of the current proposals for implementation of an electronic card system also calls for one or more databases on the other end of the medical/insurance transaction, keeping track of every claim filed and every medical treatment administered.

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

26 Sheri Alpert, op. cit., footnote 21.

27 Stuart Katsky, National Institute of Standards and Testing, personal communication, Oct. 26, 1992; OTA workshop, Dec. 7, 1992.

28 Sean McLinden, GFN Healthcare, Inc., personal communication, Mar. 14, 1993.

29 Ibid.

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

31 See, for example, Guide for Unique Healthcare Identifier Model, ASTM document, Apr. 29, 1993. The document is not an ASTM Standard. It is under consideration within an ASTM Technical committee but has not received all approvals required to become an ASTM Standard.

32 The proposal of the Bush administration before the 102d Congress, "The Medical and Insurance Information Reform Act of 1992," required use of the Social Security Number.

33 To change over to another system, it is argued by some, would be extremely costly. However, in testimony before the House Subcommittee on Social Security, Gwendolyn S. King, Commissioner of Social Security, discussed the potential effect on the Social Security Administration of expanded use of the SSN through proposals to make the Social Security card a national personal identifier. She stated that, to issue new Social Security cards containing enhancements to make them useful for personal identification would be an "enormous and expensive undertaking. The process of verifying identities and reissuing everyone a new, more secure card would be very costly–in the range of $1.5 to $2.5 billion." (This testimony did not specifically address us of the number as a unique patient identification number.) The exact cost would depend on the security features and issuance procedures used. U.S. Congress, House Committee on Ways and Means, Subcommittee on Social Security, Hearing on the Use of the Social Security Number as a National identifier, Serial 102-11, Feb. 27, 1991, pp. 24-25. Others suggest that implementation of a medical identification number could be accomplished on a prospective basis. Jeff Neuberger, Raysman & Milstein, New York, NY, personal communication, April 1993.

34 William M. Bulkeley, "Get Ready for Smart Cards and Health Care," The Wall Street Journal, May 3, 1993, p. B11.

35 U.S. Department of Health, Education, and Welfare, The Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens (Washington, DC: U.S. Government Printing Office, 1973), p. 121. The advisory committee warned that the use of the Social Security number as a personal identifier "would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems..."

36 See, A. Westin and M. Baker, Databanks in a Free Society (New York, NY: Quandrangle Books, 1972), p. 399.

37 Greidinger v. Davis, Case No. 92-1571, Decided Mar. 22, 1993, p. 17. In Greidinger, the court found that the plaintiff's fundamental right to vote was substantially burdened to the extent the statutes at issue permitted the public disclosure of his Social Security number.

38 Ibid. p. 18. The court also acknowledges that its review of potential harm is not exhaustive, but highlights some instances to illustrate the egregiousness of the harm.

39 Position statement of the American Health Information Management Association on the Universal Patient Identifier, Draft as of Aug. 8, 1993. AHIMA recommends use of the Social Security Number with the addition of an encrypted confidentiality code for use initially to link a patient's records across the health care system. Access to the patient's records would require use of both the Social Security number and the confidential code. Providers would be free to use their own system of patient identification, but the records of different providers would be linked via use of the Social Security number with an encrypted confidentiality code. For the longer term, AHIMA believes a nationwide system of biometric identifiers must be implemented.

40 This policy would be part of a greater scheme in the protection of rights to privacy in personal information, whether health care information or otherwise. Sean McLinden, op.cit., footnote 28.

41 The Ontario, Canada system provides for universal access to health care benefits.

42 Privacy advocates in the United States voice similar concerns about the Social Security number becoming a de facto national identification number through the proliferation of its use in the private sector.

43 David H. Flaherty, "Privacy, Confidentiality, and the Use of Canadian Health Information for Research and Statistics," Canadian Public Administration, vol. 35, No. 1, 1992, p. 80. Flaherty asserts that, "those seeking to strengthen the health information system need to be sensitive to the risk of unique personal identifiers being used for purposes unrelated to health that may pose serious threats to the privacy of individuals." Speaking of the Canadian system he states that "provinces must be encouraged to enact legislation to restrict the use of such health identifiers to health-related purposes, in both the public and private sectors, in order to reduce public anxieties about abuse of such numbers."

44 Institute of Medicine, op. cit., footnote 19, pp. 144- 145. U.S. Congress, General Accounting Office, Automated Medical Records: Leadership Needed to Expedite Standards Development. Report to the Chairman, Committee on Governmental Affairs, U.S. Senate; GAO/IMTEC-93-17 (Gaithersburg, MD: U.S. General Accounting Office, 1993), p. 8. General Accounting Office characterizes these categories of standards similarly, as vocabulary, structure and content, messaging, and security.

45 Some commentators believe that the responsibility of establishing and maintaining a common electronic data dictionary as well as a system of unique patient identifiers should be delegated to a Privacy Protection Board. Randall Oates, American Academy of Family Practice, personal communication, April 1993.

46 Automated Medical Records: Leadership Needed to Expedite Standards Development, op. cit., footnote 44, p. 10. The report also notes that additional standards will be needed, including those for unique patient record identifiers, access procedures, encryption approaches, identification of invalid or inaccurate data, and verification of user access privileges.

47 Ibid., p. 11. At least 15 different confidentiality committees have been formed and are working on issues related to the protection of computerized records. There appears to be, however, a wide gap in the approach and scope of different groups' efforts due to a lack of consensus on appropriate confidentiality measures and national goals. "Computerization and Confidentiality," Toward an Electronic Patient Record: Updates on Standards and Developments, vol. 1, No. 6, pp. 1-8, January 1993.

48 The American Health Information Management Association defines "medical information" 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 is

1. related to a patient's health care; or
2. is obtained in the course of a patient's 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 definition may include information beyond the confines of the patient record. In Canada, patient records usually include all recorded information within an institution relating to the health of individual patients. This would include nurses' notes, medical orders, consultation reports, laboratory reports as well as information that is recorded on other forms such as microfilm, audio and video tape, xray, etc. The information relates to the state of health of a patient prior to his admission, at various stages during his stay at the institution, or during the period in which he takes treatment or care, the opinions of those caring for or treating him relating to his state of health. It also relates to care and treatment provided, and the effect of that care and treatment. Under the Canadian system, the content of the medical record is prescribed by the laws of the province, by regulation and by the bylaws of health care facilities. Federal legislation, including the Narcotic Control Act and the Food and Drug Act, also affects the contents of medical records. Kevin P. Feehan, "Legal Access to Patient Health Records/Protection of Quality Assurance Activities," Health Law in Canada, vol. 12, No. 1, 1991, p. 3.

49 Robert M. Gellman, "Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy," North Carolina Law Review, vol. 62, No. 2, 1984, p. 258.

50 OTA Workshop, July 31, 1993.

51 Ibid.

52 David Flaherty, Professor of History and Law, University of Western Ontario, personal communication, January 1993.

53 According to Alexander Capron, informed consent serves several functions:

1. the promotion of individual autonomy;
2. the protection of patients and subjects;
3. the avoidance of fraud and duress;
4. the encouragement of self-scrutiny by medical professionals;
5. the promotion of rational decisions;
6. the involvement of the public (in promoting autonomy as a general social value and in controlling biomedical research).

Principles of Biomedical Ethics, 2d ed., Tom L. Beauchamp, James F. Childress, eds., (New York, NY: Oxford University Press, 1983) pp. 69-70.

54 The Department of Health and Human Services has promulgated regulations for consent by human subjects in medical treatment in 4 CFR Section 46.116.

55 Principles of Biomedical Ethics, 2d ed. op. cit., footnote 53, pp. 69-70.

56 Ellen Klugman, "Toward a Uniform Right to Medical Records: A Proposal for a Model Patient Access and Information Practices Statute," U.C.L.A. Law Review, vol. 30, No. 6, 1983, p. 1362.

57 The American Medical Association has stated that the"notes made in treatin g a patient are primarily for the physician's own use and constitute his personal property." Bruce Samuels and Sidney M. Wolfe, Medical Records: Getting Yours (A Consumer's Guide to Obtaining and Understanding the Medical Record) (Washington, DC: Public Citizen's Health Research Group, 1992), p. 2.

58 George J. Annas, The Rights of Patients: The Basic ACLU Guide to Patient Rights, 2d ed. (Carbondale and Edwardsville, IL: Southern Illinois University Press, 1989), p. 163. Networking of information would likely challenge these concepts of ownership, as information is transmitted between practitioner, reimburser, clinic and hospital. While patients may control initial release of identifiable information, the property right in the information may become less clear as data is subsequently transmitted between parties. Kathleen A. Frawley, Director, Washington, DC Office, American Health Information Management Association, personal communication, August 1993.

59 Klugman, op. cit., footnote 56, p. 1362.

60 Bruce Samuels and Sidney M. Wolfe, op. cit., footnote 57, p. 32. See ch. 3 of this publication for an analysis of existing rules regarding access to medical records in each of the 50 States and the District of Columbia.

61 See, e.g., Wallace v. University Hospitals of Cleveland, 82 Ohio Law Abs. 257, 164 N.E. 2d 917 (1959), modified and aff'd., 84 Ohio Law Abs. 224, 170 N.E.2d 261 (Ohio App. 1960). The lower court held that "a patient has a property right in the information contained in the record and as such is entitled to a copy of it." 164 N.E.2d at 918. On appeal, the patient's right of access was limited to those records that, in the hospital's judgment, were in the "beneficial interest" of the patient to inspect. 170 N.E.2d at 261-262.

62 The usual example of detrimental information is a fatal prognosis, a diagnosis of a malignant disease or psychiatric diagnoses.

63 It also runs contrary to the findings of some commentators on this issue. See discussion in James M. Madden, "Patient Access to Medical Records in Washington," Washington Law Review, vol. 57, No. 4, 1982, p. 697, which discusses studies concluding that "even though patients were sometimes upset by what they read, they were generally comfortable with reading their records and felt better informed and more involved in their treatment." Another study concluded that patient access to the record was helpful in allaying suspicions, developing trust, and obtaining consent for treatments Two studies, however, emphasized that knowledgeable staff should be present when patients inspect records to help interpret potentially disturbing material. The article recommends a general right of patient access to mental health records, but suggests a need to protect patients from potentially disturbing material.

64 Letter from George J. Annas, Daryl Matthews, and Leonard H. Glantz, Boston University School of Medicine and Public Health, to the New England Journal of Medicine, vol. 302, No. 26, 1980, p. 1482.

65 George Annas, op. cit., footnote 58, p. 164.

66 42 C.F.R. Part 2.

67 The Privacy Act of 1974, P.L. 579, 88 Stat. 1896, codified as 5 U.S.C. Sec. 552a.

68 U.S. Privacy Protection Study Committee, Personal Privacy in an Information Society (Washington, DC: U.S. Government Printing Office, 1977).

69 Position Statement of the American Health Information Management Association, Chicago, IL, March 1992, p. 1.

70 This limitation is recognized by others. See, James Madden, op. cit., footnote 63, 1982. The District of Columbia Mental Health Information Act takes this approach. DC Code Ann. Section 6-2076 (1981). The Act creates a general right of patient access to mental health records on request, but also provides: (1) that a mental health professional shall have the opportunity to discuss the information with the patient at the time of inspection, Id. at Section 6-2041 and that (2) information may be withheld only if the mental health professional "reasonably believes" that withholding is necessary to protect the patient from a "substantial risk of imminent psychological impairment" or to protect the patient or another individual from a "substantial risk of imminent and serious physical injury," Section 6-2042.

71 Ibid, p. 2.

72 David H. Flaherty, "Ensuring Privacy and Data Protection in Health and Medical Care," prepublication draft, p. 13.

73 Randall Oates, American Academy of Family Practice, personal communication, April 1993.

74 George Annas, op. cit., footnote 58, p. 185. Annas criticizes such general release forms as so broad and vague that the patient cannot reasonably and knowingly sign them.

75 David H. Flaherty, op. cit., footnote 72, p. 16.

76 Privacy Protection Study Committee, op. cit., footnote 68.

4 DESIGNING PROTECTION FOR COMPUTERIZED HEALTH CARE INFORMATION

Health care workers, insurers, medical records specialists, and privacy advocates believe that as computerization of health care information proceeds, new Federal legislation is needed to protect individual privacy in that information. (See footnote 1) New legislation should address not only concerns about the computerized medical record, but also health care information stored in data systems.

In these respects, new legislation for computerized health care information can be modeled on codes of fair information practices. However, new legislation should also anticipate the challenges that computerization of health care information presents with respect to possible new demands for data and linkages, creation of new databases, and changing technologies and requirements for computer security. Such legislation should also reflect technological capabilities to secure data and track data flow. It should provide for enforcement of these practices, and allow individuals redress for wrongful access and use of medical information, both in criminal and civil actions.

Based on an analysis of current State statutes and legislative models and initiatives, effective and comprehensive health care information legislation would have to do the following:

- Define the subject matter of the legislation, "health care information," to encompass the full range of information collected, stored, and transmitted about individuals, not simply the content of the medical record.
- Define the elements that constitute violation of health care information privacy and provide criminal and civil sanctions for improper possession, brokering, disclosure, or sale of health care information with penalties sufficient to deter perpetrators.
- Establish requirements for informed consent.
- Establish rules for educating patients about information practices; access to information; amendment, correction, and deletion of information; and creation of databases.
- Establish protocols for access to information by secondary users, and determine their rights and responsibilities in the information they access.
- Structure the law to trace the information flow, incorporating the ability of computer security systems to warn and monitor leaks and improper access to information so that the law can be applied to information at the point of abuse, not just to one "home" institution.

- Establish a committee, commission, or panel to oversee privacy in health care information.

While no single proposal or scheme for data protection adequately addresses all of the needs of a health care information protection system, many offer models on which health care information legislation might be based. This chapter examines principles of fair information practices, and their strengths and limitations in protecting privacy in computerized health care information. It then discusses specific data protection initiatives (see box 4-A and discussion below) and the applicability of their provisions to the needs of health care data protection. This discussion also includes aspects of proposals made by experts in computer privacy issues and certain legislative initiatives.

4.1 FAIR INFORMATION PRACTICES AND THE PRIVACY ACT

Proposals for protection of personal health data, whether maintained on computers or otherwise, have largely been based on a system of fair information practices. These proposals have been suggested by such organizations as the American Health Information Management Association and the American Medical Association. The Uniform Health Care Information Act (UHCIA) and systems for treating specific kinds of health care information, such as the provisions of the Massachusetts code are also applicable. (For a discussion of several initiatives for protection of privacy in health care information, see box 4-A. The full texts of these initiatives are in Appendix B.) The basic principles of fair information practices were stated in Computers and the Rights of Citizens, a report published by the U.S. Department of Health, Education and Welfare in 1973. The report identified five key principles:

1. There must be no secret personal data record-keeping system.
2. There must be a way for individuals to discover what personal information is recorded and how it is used.
3. There must be a way for individuals to prevent information about them, obtained for one purpose, from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of information about themselves.
5. An organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuses of the data.

These principles are clearly evident in the provisions of the Privacy Act of 1974 ("Privacy Act"), which "adopts the accepted privacy principles as policy for Federal agencies." The law gives individuals the right to access much of the personal information about them kept by Federal agencies. It places limits on the disclosure of such information to third persons and other agencies. It requires agencies to keep logs of all disclosures, unless systems of records are exempt from the Privacy Act. (See footnote 2)

The Federal Privacy Act also gives an individual the right to request an amendment of most records pertaining to him or her if he or she believes them to be inaccurate, irrelevant, untimely, or incomplete. (See footnote 3) The agency must acknowledge the request in writing within 10 days of its receipt. It must promptly (no time limit is specified) make the requested amendment or inform the individual of its refusal to amend, the reasons for the refusal, and the individual's right to request a review by the agency head. If the individual requests such a review, the agency head has 30 days to render a decision. Should the agency head refuse to amend the information, the individual can file a concise statement of his disagreement with the agency decision. There after, the agency must note the dispute in the record and disclose this fact, along with the individual's statement, whenever the record is disclosed.

The Federal Privacy Act further provides that the individual can pursue his disagreement, and indeed any noncompliance by an agency, with a civil suit in Federal District Court. He or she can obtain an injunction against a noncomplying agency, collect actual damages for an agency's willful or intentional noncompliance, and be awarded attorney's fees and costs if he or she "substantially prevails" in any such action. Agency personnel are criminally liable for willful noncompliance; the penalty is a misdemeanor and a fine of up to a $5,000.

The Federal agencies also have a responsibility to collect only relevant information on individuals, to get the information directly from the individual whenever possible, and to notify the individual of several facts at the time the information is requested. Willful failure to comply with the notification requirement may result in civil and criminal liability.

The Privacy Act also covers agencies' "systems of records" and requires an annual, nine- point report to be published in the Federal Register. The report must contain information such as categories of records maintained; their routine use; policies on their storage and retrieval; and other agency procedures relating to the use, disclosure, and amendment of records. Agencies also have extensive rule-making duties to implement each component of the law.

The Act is limited, however, in several significant ways. Some believe that a system of notification through the Federal Register is cumbersome and burdensome to the individual who, practically speaking, does not regularly review the register, so that notification is not effective. The Act also places the burden of monitoring privacy in information and redressing wrongs entirely with the individual, providing no government oversight mechanism for the system.

In addition, the Act itself is limited in its application to "routine use" of the record, which refers to disclosure of records, not how the collecting agency uses those records internally. Many commentators have noted that the penalties prescribed in the Act are inadequate, (see footnote 4) and others comment that the Act contains no specific measures that must be in place to protect privacy so that it cannot be used to describe what technical measures must be taken to achieve compliance. (See footnote 5)

Fair information practices and the provisions of the Privacy Act form the bases for most initiatives to protect medical information. Characteristics common to these proposals are:

1. They pertain to 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 a government entity requests personal information from an individual, laws require the individual to be notified of 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 amend ment.
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 disagree ment, which must be included in the record and disclosed along with it thereafter.
9. The individual can seek review of a denied request.

An earlier OTA report, Electronic Record Systems and Individual Privacy (1986) (see footnote 6), noted that the Privacy Act of 1974 did not consider the distributed processing, sophisticated database management systems, computer networks, and the wholesale use of microcomputers that will be used for medical information. To the extent that medical information protection is based solely on the Privacy Act and principles of fair information practices, it fails to consider these developments and the complexity of current computer network technology. It is apparent that protecting personal information in a computerized environment involves, at minimum, access to records, security of information flows, and new methods of informing individuals of where information is stored, where it has been sent, and how it is being used (see box 4-A).

4.2 FEATURES OF HEALTH CARE PRIVACY LEGISLATION

Congress has acted in other areas to protect the confidentiality of nongovernmental records. The Right to Financial Privacy Act, (see footnote 7) the Family Educational Rights and Privacy Act of 1974 (popularly known as the Buckley Amendment) (see footnote 8) to protect the privacy of records maintained by schools and colleges, the Fair Credit Reporting Act (see footnote 9) to protect the privacy of consumers in the reporting of credit information, and the Federal Videotape Privacy Protection Act (see footnote 10) all serve this purpose. In addressing concerns about the privacy of health care information through legislation, Congress may wish to make the following provisions:

Provision 1: Define the subject matter of the legislation, "health care information" to encompass the full range of medical information collected, stored, and transmitted about individuals, not simply the medical record.

"Appropriate data protection should. . .cover the entire range of personal data systems involved in health care, not just the clinical record used for primary treatment." (see footnote 11) This assertion reflects the broad range of identifiable personal information maintained in health care settings, including administrative, clinical, diagnostic, educational, financial, laboratory, psychiatric, psychosocial, quality control, rehabilitative, research, risk management, social service, and therapeutic records. (See footnote 12) To be effective, legislative protection of "health information" should address the full scope of this information.

The Ethical Tenets for Protection of Confidential Clinical Data ("Ethical Tenets") define the subject of protection, "clinical data" as including "all relevant clinical and socioeconomic data disclosed by the patient and others, as well as observations, findings, therapeutic interventions and prognostic statements generated by the members of the healthcare team." Legislative proposals, however, define health care information in different ways. The Model State Legislation on Confidentiality for Health Care Information of the American Medical Association refers to "confidential health care information," defining it 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 language of this legislation is particularly helpful because it provides that health care records be recognized by law when in electronic form.

The American Health Information Management Association's (AHIMA's) Health Information Model Legislation, while also defining "health care information" broadly, specifically refers to it as data or information, whether oral or recorded in any form or medium, that can be associated with the identity of a patient or other record subject; and–

- relates to a patient's health care; or
- is obtained in the course of a patient's 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 language acknowledges health care information in its broadest terms as being information relating to or collected in the course of a patient's health care, and does not limit it to where it resides. Arguably, health care information (be yond the contents of the medical record) located in such places as student files, pharmacy computers, public health agencies, and lawyers offices is covered by this definition. The scope of AHIMA's proposed legislation would provide coverage to information as it flows through a complex computer network through which it is accessed by a variety of primary and secondary users.

Provision 2: Define the elements comprising invasion of privacy of health care information, and provide criminal and civil sanctions for improper possession, brokering, disclosure, or sale of health care information with penalties sufficient to deter perpetrators.

The Massachusetts law on Insurance Information and Privacy Protection provides that a person who knowingly and willfully obtains information about an individual from an insurance institution, insurance representative, or insurance-support organization under false pretenses shall be fined not more than $10,000 or imprisoned not more than 1 year, or both.

The Privacy Act provides guidelines to address the problem of information brokering and abuse of information accessed by authorized persons within a data system. (See footnote 13) The Act provides criminal sanctions for officers or employees of an agency who have possession of or access to records that contain individually identifiable information that may not be disclosed under the provisions of the Privacy Act. If a person discloses the material to any person not entitled to receive it, he or she is guilty of a misdemeanor and subject to a fine of up to $5,000. Similar sanctions apply when an officer or employee of an agency willfully maintains a system of records without satisfying notice requirements, or when a person requests or obtains any record of an individual from an agency under false pretenses. (See footnote 14)

The Uniform Health Care Information Act, which has been enacted into law in Montana and Washington, provides criminal sanctions for illegally obtaining health care information. Persons obtaining health care information maintained by a health care provider by means of bribery, theft, or misrepresentation of identity, purpose of use, or entitlement to the information are guilty of a misdemeanor under the Act. Persons found guilty are subject to criminal penalties of imprisonment for not more than 1 year, or a fine not exceeding $10,000, or both. A person presenting a false disclosure authorization form or certification to a health care provider is also guilty of a misdemeanor and is subject to similar criminal penal ties. Civil recourse is available to persons harmed by the violations under the Act. The court may award damages for pecuniary losses and punitive damages if the violation results from willful or grossly negligent conduct. The court may also assess attorney's fees.

The Federal Privacy of Medical Information Bill of 1980 (which was not enacted into law) prohibited requesting or obtaining access to medical information about a patient from a medical care facility through false pretenses or theft. It imposed higher penalties on those who did so for profit or monetary gain. The bill also authorized civil suits for actual and punitive damages and equitable relief against officers and employees of Federal and State governments, by any patients whose rights had been knowingly and negligently violated.

The AHIMA Model Legislation provides that anyone who requests or obtains health care information under false or fraudulent pretenses is subject to a $10,000 fine or imprisonment for 6 months. Anyone who obtains health care informa tion fraudulently or unlawfully and intentionally uses, sells, or transfers the information for some monetary gain is subject to fines of not more that $50,000 and imprisonment for 2 years. The AHIMA Model Legislation also provides for civil remedies and monetary penalties. Among the civil money penalties provided for is a fine of not more that $1,000,000 if it is found that violations of the provisions have occurred in such numbers or with such frequency as to constitute a general business practice. In the discussion about health care information privacy, commentators and stake holders indicate that for legislation to be mean ingful, penalties for improper access, possession, brokering, disclosure, or sale of information must be stringent enough to deter perpetrators. (See footnote 15) Provisions or penalties such as those set forth in the AHIMA Model Legislation might be more likely to deter information brokers who might otherwise include fines and penalties in their cost of doing business.

Provision 3: Establish requirements for informed consent.

The Massachusetts law on Insurance Information and Privacy Protection details the required elements for disclosure authorization forms used in connection with insurance transactions. The provisions for disclosure authorization set forth in this statute are applicable to requirements for informed consent of health care information generally. According to the Massachusetts law, the disclosure authorization form must (1) be written in plain language; (2) be dated; (3) specify the types of persons authorized to disclose information about the individual; (4) specify the nature of the information authorized to be disclosed; (5) name the institution to whom the individual is authorizing information to be disclosed; (6) specify the purposes for which the information is collected; (7) specify the length of time authorization shall remain valid; and (8) advise the individual, or a person authorized to act on behalf the individual, that the individual or his authorized representative is entitled to receive a copy of the authorization form. (See footnote 16)

Provision 4: Establish rules for educating patients about information practices; access to information; amendment, correction and deletion of information, and creation of databases.

The Privacy Act contains specific provisions about the right of access of individuals to records maintained by a Federal agency. The Act establishes agency requirements for maintenance and collection of information. Agencies maintaining records must limit the information collected to that which is relevant and necessary to accomplish the stated purpose. Individuals who supply information to an agency must be informed as to the purpose of the information, the uses that may be made of the information, who authorized the collection of the information, and the effects on the individual of not providing the requested information. An agency is required to make public a notice of the existence and character of the system. (See footnote 17) Only a notice in the Federal Register is required by the Privacy Act, which many believe does not adequately inform the patient population about information uses and practices.

By contrast, under the Massachusetts law on Insurance Information and Privacy Protection, insurers are obligated to provide a description of information practices to applicants and policy- holders when applying for coverage and renewing or reinstating policies. The notice must include:

1. whether personal information may be collected from persons other than the individual proposed for coverage;
2. the type of personal information that may be collected and the sources and investigative techniques that may be used to collect it;
3. the type of disclosure without authorization that is permitted by the law and the circumstances under which the disclosure may be made; and
4. information about patient rights to access, amend, correct, and delete information.

This law provides for individuals to access information maintained about themselves by insurers. It also provides that an individual has a right to have factual errors corrected and any misrepresentation or misleading entry amended or deleted. The statute states that within 30 business days from receipt of a written request to correct, amend, or delete any personal information that their insurer shall either do so or reinvestigate the disputed information and notify the individual of the grounds for refusing the request. The insurer must also notify persons and institutions that have received or provided the information. When a correction is not made, the subject is permitted to file a statement setting forth what he or she believes to be is the correct, relevant, or fair information, and provide a statement of reasons why he or she disagrees with the insurer's refusal to change it.

The Ethical Tenets also provide for access by the patient to health care information maintained in his or her file. Like the Massachusetts code, they require that patients be involved and informed about the recordkeeping process. Patients are deemed owners of the information provided during the course of the medical care as well as of the clinical data related to clinical care. (See footnote 18) Patients must be kept informed of the location, practices, and policies for information maintained in electronic medical data. The Ethical Tenets define "kept informed" as providing a description and explanation of the record storage and access rules and exceptions defined in the operating policies of data centers. The Tenets require that these policies be explained to the patients, including the basic rule that patients are the owner of their own records, and should describe the exceptions such as "regulatory agency functions," or in the case of emergency, the authorization of the data center's security officer to release "key data" to the attending physician. Patients must be notified of special authorizations, such as those for researchers seeking clinical information that in cludes patient identifiers. (See footnote 19)

The Uniform Health Care Information Act (UHCIA) also requires that a health care provider inform the patient about information practices, including a notice that is to be posted in the health care facility that states:

> We keep a record of the health care services we provide for you. You may ask us to see and copy that record. You may also ask us to correct that record. We will not disclose your record to others unless you direct us to do so or unless the law authorizes or compels us to do so. You may see your record or get more information about it at. . . .(see footnote 20)

The UHCIA sets forth the requirements and procedures for the patient's examination and copying of his or her record. Within 10 days of a patient's request, the provider must make the information available for examination or provide a copy to the patient, or inform the patient that the information does not exist, cannot be found, or is not maintained by the provider. Special provisions cover delays in handling the request, and the provider's obligations in providing explanations of codes or abbreviations. Providers can also deny the request; the statute sets forth the circumstances under which they may do so. These include when the health care information would be injurious to the health of the patient, when it might endanger the life or safety of an individual, or when it might lead to the identification of an individual who provided information in confidence. Special provisions are made for access to health care information by a patient who is a minor.

Special provisions are made for requests for correction or amendment of a record by a patient for purposes of accuracy or completeness. When a request is made, the provider must make the correction; inform the patient if the record no longer exists or cannot be found; make provisions for making the changes if there is a delay; or inform the patient in writing of the provider's refusal to correct or amend the record as requested, the reason for the refusal, and the patient's right to add a statement of disagreement and to have that statement sent to previous recipients of the disputed health care information. Specific procedures for making changes to the record are also provided for.

Provision 5: Establish protocols for access of information by secondary users, and determine their rights and responsibilities in the information they access.

The Ethical Tenets address the handling of data by secondary users referred to as a "secondary clinical record"; i.e., the data derived from the primary patient record for administrative, fiscal, epidemiologic, and other purposes outside the primary patient/provider relationship. According to the Tenets, these records are created for a "limited purpose, are not a part of the patient's treatment, and not a part of the professional communication to contribute to the care of the patient." For instance, a physician may be required to report information to an insurance company to assess a disability. The Tenets provide that "[i]dentified secondary clinical records shall receive confidential treatment"– i.e., those records including patient identifiers such as name, address, telephone number, or Social Security number. (See footnote 21)

The Ethical Tenets provide that identified secondary records are to be used only for the purpose for which they were provided, and specifically require that they be destroyed or masked as promptly as possible once the task is accomplished. The Ethical Tenets provide for release of data for public health or research purposes. If the release of primary or secondary data is deemed desirable or appropriate for these purposes, patients must grant informed consent and formal authorization before information will be released.

Trubow (see footnote 22) suggests specific obligations for secondary users of personal information. The holder of a record should notify the data subject about the records in his or her possession or control. The recordholder should:

1. disclose the purpose for which the information was collected;
2. explain the primary and parallel uses of the information;
3. provide to the individual subject a procedure to examine, challenge, and correct the information; and
4. give the individual an opportunity to deny any designated parallel uses.

Trubow recommends that the record-holder be allowed to use the information only for those uses of data to which the individual subject has been notified and not to which he or she has objected. The record-holder may not make any secondary use of personal information without the individual's express consent. These notice requirements, coupled with provisions similar to those of the Ethical Tenets for destruction of information after use, would adequately notify the individual subject about use of other data and could reduce the probabilities of creating new databanks of health care information outside the patient/provider relationship.

Provision 6: Structure the law to track the information flow, incorporating the ability of computer security systems to monitor and warn of leaks and improper access to information so that the law can be applied to the information at the point of abuse, not to one "home" institution.

Existing legislation and proposals for protection of health care information place responsibility for data protection on each institution. As discussed in chapter 2, the ability to transfer and exchange information among institutions so that there is no single point of origination or residence for the information makes such an approach unworkable. Legislation should take advantage of the technological ability to track data flows and maintain auditing records of each person who accesses information, at what location, and at what time. (See discussions of computer security measures in ch. 3 and Appendix A.) Monitoring information access and abuse in this way allows the flexibility needed to monitor all institutions and users along the chains of access.

The Canadian Commission d'Acces a l'Information issued a specific set of minimum requirements for the security of computerized health care records. The commission indicated that its mandatory rules on health care information applied to mainframe computers, the machines of the suppliers of computer services, and to microcomputers. In addition to the designation of a responsible person to implement and enforce security measures and maintain their currency (preferably with the assistance of a committee), it prescribed, in detail, technical procedures for user identification and authentication, and the creation of "access profiles" for the type of personal information specific users need to perform their duties. The rules further prescribe for such matters as site security and audit trails. Application of such a set of minimum requirements to institutions using health care information would enable tracking of information flow and access and allow for shared responsibility to protect health care information among institutions using it.

Brannigan's approach to protecting privacy in clinical information is through the use of "technical tools." (See footnote 23) These tools include both "machine-based" and "people-based" precautions, including concepts such as "need to know," encryption, audit trails, read/write limitations, physical keys, and passwords. (See footnote 24)

Brannigan looks to the National Practitioner Data Bank (NPDB), a large computer system operated by UNISYS as a contractor to the Public Health Service. NPDB operates by collecting reports on physicians submitted by authorized reporters, consolidating them and sending them, on request, to authorized institutions.

The NPDB process would be analogous to a single request for a patient's entire computer- based medical record, as opposed to a clinical inquiry on a specific visit. As such, it makes a reasonable technical analogy to the proposed transmission of computer-based medical records.

Confidentiality of the data is a major concern. After analyzing the technical data protection tools in the NPDB and identifying discontiniuties in the system, Brannigan set forth a list of technical provisions needed for a reasonably secure multi- institutional system for sharing patient records:

1. control authorized requesters by use of restricted request software needed to access the database;
2. protect passwords used to identify individual requesters;
3. route requests through a secure electronic mail system that eliminates direct electronic connection to the data bank;
4. allow searches only by patient name, and prevent random browsing of the data bank;
5. provide an audit trail to the individual subject;
6. maintain a secure data facility not connected to the health institution;
7. allow responses to be sent in a secure manner, only to pre-approved addresses; and
8. provide the individual subject a way to monitor disputed, incorrect, or unneeded data.

   In addition, the system might include:

9. encryption and transmission through secure electronic mail to a mailbox accessible only to users with authorized decryption software;
10. permit searches only for authorized purposes; and
11. searches allowed only with the permission of that patient. (See footnote 25)

Industry established standards, as discussed in chapter 3, could also be incorporated into legislation. Compliance with technical requirements for assuring confidentiality could be required by law, with sanctions for failure to meet standards.

Provision 7: Establish a committee, commission, or panel to oversee privacy in health care information.

One approach to addressing the problem of maintaining privacy in computerized medical records is the establishment of a committee on health care information privacy. Such a committee could be modeled in some aspects on proposals for a data protection board. (See footnote 26) Legislation alone cannot address all of the privacy problems created as a result of quickly changing and developing computer technology. A committee could serve a more dynamic function and could assist in implementing the health care information privacy policies set out in legislation. Data protection boards have been instituted in several foreign countries, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Iceland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia. (See footnote 27)

The responsibilities and functions suggested for a data protection board are particularly applicable to the issues of health care information privacy and can be implemented in the following ways. A health care information privacy committee could:

1. identify health care information privacy concerns, functioning essentially as an alarm system for the protection of personal privacy;
2. carry out oversight to protect the privacy interests of individuals in all health care information-handling activities;
3. develop and monitor the implementation of appropriate security guidelines and practices for the protection of health care information;
4. advise and develop regulations appropriate for specific types of health care information systems. (Staff members of such a committee could thus become specialists in different types of health care information systems and information flows);
5. monitor and evaluate developments in information technology with respect to their implications for personal privacy in health care information; and
6. perform a research and reporting function with respect to health care information privacy issues in the United States.

As part of its responsibilities, the health care information privacy committee could also monitor the establishment and use of computer systems for health care data in the private sector, and make recommendations on the potential expansion of the content of the medical records and different uses of health care data. The committee could closely watch the progress of the technology for health care data and storage, and track the development of technical capabilities and security measures.

A committee could help avoid the need to deal with privacy problems "after the fact," that is, after new uses have been established for data and new inroads made into individual privacy in health care information, by taking a prospective approach to addressing privacy concerns. Some suggestions have been made that a committee of this type be established within a division of the Department of Health and Human Services. Others suggest that this such a committee operate independently from any Federal agency. (See footnote 28)

4.3 FOOTNOTES

1 OTA Workshop, "Designing Privacy in Computerized Medical Information," Dec. 7, 1992.

2 Other Federal policy on the right to access government information is set forth in the Federal Privacy Act at 5 U.S.C. Sec. 552, which deals with public information and public access to agency rules, opinions, orders, records, and proceedings.

3 The Privacy Act exempts from this provision records pertaining to law enforcement. Public Law 93-579 Sec. 552a(k)(2).

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

5 Vincent M. Brannigan, "Protecting the Privacy of Patient Information in Clinical Networks: Regulatory Effectiveness Analysis," Extended Clinical Consulting by Hospital Computer Networks, D.F. Parsons, C.N. Fleischer, and R.A. Greene, eds. (New York, NY: Annals of the New York Academy of Sciences, 1992) vol. 670, pp. 190-201.

6 OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

7 Public Law 95-630, title XI, 92 Stat. 3697, Nov. 10, 1978, et seq.

8 Public Law 93-380, title V, Sec. 513, 88 Stat. 571, Aug. 21, 1974.

9 Public Law 91-508, title VI, Sec. 601, 84 Stat. 1128, Oct. 26, 1970, et seq.

10 Public Law 100-618 Sec. 2(a)(1),(2), 102 Stat. 3195, Nov. 5, 1988 et seq.

11 David H. Flaherty, "Ensuring Privacy and Data Protection in Health and Medical Care," prepublication draft, Apr. 5, 1993.

12 Ibid.

13 Discussion of these activities in the context of computerized medical information is discussed in ch. 2. Further discussion about the Privacy Act generally is also found in ch. 2.

14 5 U.S. Code, Sec. 552a(h). Many commentators believe that these penalties are inadequate to address information abuses. Joan Turek-Brezina, op. cit., footnote 4.

15 OTA workshop, "Emerging Privacy Issues in the Computerization of Medical Information," July 31, 1993.

16 The code also makes specific provisions for the length of time such disclosure authorization remains valid.

17 The notice must include the system's name and location, the categories of records maintained on the system, the categories of individual on whom records are maintained in the system, each use of the record contained in the system, and the policies. The Act provides that when an agency refuses to amend an individual's record or refuses to grant an individual access to his or her record, civil action may be brought. The court will order the agency to comply with the provisions of the Act, and will require the government to pay attorneys' fees and litigation costs. In cases when an agency fails to properly maintain an individual's record according to the provisions of the Act, damages of at least $10,000 will be awarded. 5 U.S. Code, Sec. 552(a); Public Law 93-579, Sec. 552a(g).

18 The Tenets make the distinction that the physician is deemed owner of the information generated by him or her during the course of medical care, such information including diagnostic, therapeutic, or prognostic comments; opinions, decision explanations, and choice rationale–all parts of the clinical reasoning and professional interpretation of the data collected. This provision addresses concerns about professional privacy. Other health care workers may be included under this protection.

19 The Federal Privacy of Medical Information Act (H.R. 5935), introduced before the 96th Congress in 1980, provided that a medical care facility shall, on request, provide any individual with a copy of the facility's notice of information practices and shall post in conspicuous places in the facility such notice or a statement of availability of such notice and otherwise make reasonable efforts to inform patients (and prospective patients) of the facility of the existence and availability of such notice. Sec. 113(b).

20 The Federal Privacy of Medical Information of 1980 (H.R. 5935) proposed a similar notification practice. In Sec. 113, it provided: A medical care facility shall prepare a written notice ofinformation practices describing:

1. the disclosures of medical information that the facility may make without the written authorization of the patient;
2. the rights and procedures . . . including the right to inspect and copy medical information, the right to seek amendments to medical information, and the procedures for authorizing disclosures of medical information and for revoking such authorizations; and
3. the procedures established by the facility for the exercise of these rights.

21 Under these provisions, the identified secondary record also refers to unique identifiers of the care-providing physician, healthcare team, and institution, which are also entitled to the right to privacy under the Tenets.

22 George B. Trubow, "Protocols for the Secondary Use of Personal Information," Report of the Roundtable on Secondary Use of Personal Information, The John Marshall Law School Center for Informatics Law, Chicago, IL, prepublication draft, Feb. 22, 1993.

23 Vincent M. Brannigan, op. cit., footnote 5.

24 Brannigan notes that one characteristic of these tools is that they can pre-exist any legal structure or be established as the result of one. "[T]he legal system can either follow or force a technology." Ibid.

25 Vincent M. Brannigan, "Protection of Patient Data in Multi-Institutional Medical Computer Networks: Regulatory Effectiveness Analysis," to be published in Proceedings of the 17th Annual Symposium of Computer Applications in Medicine Care, November 1993.

26 Such a board was supported by the Office of Technology Assessment in its 1986 study of Electronic Record Systems and Individual Privacy. In its discussion of the issue, OTA cited the lack of a Federal forum in which the conflicting values at stake in the development of Federal electronic systems could be fully debated and resolved.

27 Kevin O'Connor, "Information Privacy: Explicit Civil Remedies Provided," Law Society Journal, March 1990, pp. 38- 39. In his article, "Protocols for the Secondary User of Personal Information," Professor George Trubow voiced the opinion of participants in a roundtable discussion of the issue convened by the Center for Informatics Law at the John Marshall Law School in Chicago that an independent Federal and/or State oversight agency, similar to European models, would be necessary to issue regulations more specifically identifying information practices and to process complaints of noncompliance. Op. cit., footnote 22.

28 OTA Workshop, op. cit., footnote 1.

APPENDIX A: SELECTED TOPICS IN COMPUTER SECURITY

Originators of existing computer-based patient record systems have been faced with the problem of ensuring their systems will provide high levels of clinical access and utility for their personnel and still maintain the security and confidentiality of patient information. Data security and confidentiality remain a central concern as the health care industry contemplates full automation and implementation of a networked computer system for individual health care information. (See footnote 1) The need for information security and trust in health care information computer systems, as in computer systems generally, is described in terms of three fundamental goals: confidentiality, integrity, and access. (See footnote 2) Confidentiality involves control over who has access to information. Integrity assures that information and programs are changed only in a specified and authorized manner, that computer resources operate correctly and that the data in them is not subject to unauthorized changes. A system meeting standards for access allows authorized users access to information resources on an ongoing basis. (See footnote 3) The level of security provided may vary from one application to another. (See footnote 4) For example, security in computer systems containing classified national security information may have different specifications than a computer system designed for a non-defense manufacturing company. Security in health care information systems would likely be designed somewhere along this spectrum. The emphasis given to each of the three requirements (confidentiality, integrity, and access) depends on the nature of the application. An individual system may sacrifice the level of one requirement to obtain a greater degree of another. For example, to allow for increased levels of availability of information, standards for confidentiality may be lowered. Thus, the specific requirements and controls for information security can vary. (See footnote 5) Applications linked to external systems will usually require different security controls from those without such connections because access is more open.

A security policy is the framework within which an organization, e.g., a hospital, outpatient clinic, mental health facility, or health insurance company, establishes needed levels of information security to achieve, among other things, the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organizational commitment for a system. It is a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (See footnote 6) A policy is implemented by taking action guided by management control principles and utilizing specific security standards, procedures, and mechanisms. (See footnote 7) A security policy, to be useful, must state the security need (e.g., for confidentiality–that data shall be accessed only by authorized individuals) and also address the circumstances under which that need must be met through operating standards. Institutions must access the threats to a system, assign a level of concern to each, and state a policy in terms of which threats are to be addressed. (See footnote 8)

Management controls are administrative, technical, and procedural mechanisms that implement a security policy. Some management controls are concerned with protecting information and information systems, but the concept of management controls is more than merely a computer's role in enforcing security. Management controls are exercised by users as well as managers. An effective program of management controls is necessary to cover all aspects of information security, including physical security, classification of information gauged to the desired levels of confidentiality and access, means of recovering from breaches of security, and training to instill awareness and user acceptance. There are trade-offs among controls. If technical controls are not available, procedural controls might be used until a technical solution is found. (See footnote 9) Nevertheless, technical controls are useless without procedural controls and robust security policy.

Breaches in security sometimes occur by outside sources, but most often by "insiders"–individuals authorized to use the system. According to the report of the Workgroup for Electronic Data Interchange to the Secretary of the U.S. Department of Health and Human Services, the Health Care Financing Administration (HFCA) believes that the security technology available to systems developers is adequate to protect against breaches by an outside source, and does not consider a breach of the system by outsiders a great concern. HFCA's concern lies with breaches of the system by "insiders," individuals who are authorized to use the system. (See footnote 10) Access control alone cannot prevent violations of the trust people and institutions place in individuals. Inside violations have been the source of much of the computer security problem in industry. Technical security measures may prevent people from doing unauthorized things, but cannot prevent them from misusing the capabilities with which they are entrusted to allow them to perform their job function. Thus, to prevent security problems resulting from violations of trust, one must depend primarily on human awareness of what others in an organization are doing and on separation of duties, as in regular accounting controls. (See footnote 11) But even a technically sound system with informed, watchful management and responsible users is not free of vulnerabilities. The risk that remains must be managed by auditing, backup, and recovery procedures supported by alertness and creative responses. Moreover, an organization must have administrative procedures in place to bring suspicious actions to the attention of responsible persons who can–and will–inquire into the appropriateness of such actions. (See footnote 12) In addition to these precautions, damage can also be avoided through close personnel checks to avoid hiring employees with questionable backgrounds in areas where sensitive data are available, periodic analysis of the computer system and the sensitivity of its data, and separation of critical duties between employees.

4.3.1 Technical Safeguards

Technical safeguards, along with administrative and procedural measures, are best established within the system application or program, e.g., medical record system software, instead of relying on the network infrastructure for security. These technical provisions include the following:

Cryptography: can be used to encode data before transmission or while stored in a computer, provide an electronic signature and/or to verify that a message has not been tampered with. Cryptography can be used to 1) encrypt plain text to provide confidentiality 2) authenticate a message to ensure integrity and to prevent fraud by third parties, and 3) create a digital signature that authenticates a message and protects against fraud or repudiation by the sender. (See footnote 13)

Personal identification and user verification techniques: help ensure that the person using a communication or computer system is the one authorized to do so and, in conjunction with access control systems and other security procedures, that authorized users can be held accountable for their actions.

Access control software and audit trails: can help protect information systems from unauthorized access and keep track of each user's activities.

Computer architecture: may be specifically designed to enhance security.

Communications linkage safeguards: can hamper unauthorized access to computers through phone lines or other networks. (See footnote 14)

4.4 CRYPTOGRAPHY

Cryptography is one method of protecting data vulnerable to unauthorized access and tampering. Cryptography, along with electronic signatures, can be used to protect confidentiality and integrity.

Confidentiality of information can be provided through encryption. Encryption (see footnote 15) is a process of encoding a message so that its meaning is not obvious; decryption transforms an encrypted message back into its normal form. (See footnote 16) When a message is encrypted, it is encoded in a way that can be reversed only with the appropriate key. (See footnote 17) Maintaining confidentiality requires that only authorized parties have the decrypting key.

Integrity can be provided through message authentication. An "authentic" message is one that is not a replay of a previous message, has arrived exactly as it was sent (without errors or alterations), and comes from the stated source (not forged or falsified by an impostor or fraudulently altered by the recipient). Encryption algorithms can be used to authenticate messages, but encryption in itself does not automatically authenticate a message.

Message authentication techniques are based either on public or secret knowledge. Authentication techniques based on public knowledge can check againsterrors, but not against malicious modifications. Message authentication using secret parameters means that a message cannot be forged unless the secret parameters are compromised or one of the parties is doing the forging.

Digital Signatures–The trend away from paper- based systems into automated electronic systems has brought about a need for a reliable, cost-effective way to replace the handwritten signature with a digital signature. Encryption or message authentication alone can only safeguard against the actions of third parties. They cannot fully protect one of the communicating parties from fraudulent actions by any other, such as forgery or repudiation of a message or transaction. Nor can they resolve contractual disputes between two parties. Like a handwritten signature, a digital signature can be used to identify and authenticate the originator of the information. A digital signature can also be used to verify that information has not been altered after it is signed, providing for message integrity.

In August 1991, NIST proposed the Digital Signature Standard (DSS) as a Federal Information Processing Standard (FIPS), suitable for use by corporations, as well as civilian agencies of the government. The DSS specifies a Digital Signature Algorithm (DSA) for use in computing and verifying digital signatures. NIST suggests that DSA can be used in such applications as electronic mail systems, legal systems, and electronic funds transfer systems. Some controversy surrounds NIST's choice of the DSS techniques. (See footnote 18)

Encryption Algorithms–The original form of a message is known as plaintext, and the encrypted form is called ciphertext. Messages are encrypted using mathematical algorithms implemented in hardware or software, and secrecy is provided through use of cryptographic keys. These keys are seemingly random sequences of symbols. The encryption algorithm is a mathematical process that can transform plain text into ciphertext and back again, with each transformation depending on the value of the key. Symmetric ciphers use the same key for encryption and decryption. One key, known to both the sender and receiver of a message, is used to both encrypt and decrypt the message. Symmetric keys present problems of key distribution, since secrecy in the key must be maintained by both parties to the communication. The traditional means of key distribution–through couriers– places the security of the cipher system in the hands of the courier(s). Courier-based key distribution presents challenges when keys need to be changed often.

Asymmetric ciphers use different but related keys. One key is used to encrypt and another to decrypt a message. (See footnote 19) A special class of asymmetric ciphers are public-key ciphers, in which the "public" encrypting key need not be kept secret to ensure a private communication. Rather, Party A can publicly announce his or her public key, PKA, allowing anyone who wishes to communicate privately with him or her to use it to encrypt a message. Party A's "secret" decrypting key (SKA) is kept secret, so that only A or someone else who has obtained his or her decrypting key can easily convert messages encrypted with PKA back into plaintext.

Determining the secret decrypting key is difficult, even when the encrypted message is available and the public key is known; in practice only authorized holders of the secret key can read the encrypted message. If the encrypting key is publicly known, however, a properly encrypted message can come from any source, and there is no guarantee of its authenticity. It is thus crucial that the public encrypting key be authentic. An impostor could publish his or her own public key, PKI, and pretend it came from A in order to read messages intended for A, which he or she could intercept and then read using his or her own secret key, SKI.

Therefore, the strength of a public key cipher system rests on the authenticity of the public key. A public key system can be strengthened by providing means for certifying public keys via digital signature, a trusted third party, or other means. (See footnote 20)

Techniques for encrypting messages based on mathematical algorithms vary widely in the degree of security they provide. The various algorithms differ in the following ways:

- The mathematical sophistication and computational complexity of the algorithm itself. More complex algorithms may be harder for an adversary to break.
- Whether the algorithm is for a symmetric cipher or for an asymmetric one.
- The length of the key used to encrypt and decrypt the message. Generally, for an algorithm of a given complexity, longer keys are more secure.
- Whether the algorithm is implemented in software or hardware.
- Whether the algorithm is open to public scrutiny. While some argue that users have more confidence in an algorithm if it is publicly known and subject to testing, the National Security Agency and others assert that secret algorithms are more secure. (See footnote 21)

Data Encryption Standard (DES)–The U.S. Data Encryption Standard (DES) is a well-known example of a symmetric cryptosystem and probably the most widely known modern encryption algorithm. DES was developed to protect unclassified computer data in Federal computer systems against passive and active attacks in communication and computer systems. (See footnote 22) DES is the result of a National Bureau of Standards initiative to create an encryption standard. Based on an algorithm developed by IBM, DES was officially adopted as a Federal Standard in November, 1977, and endorsed by the National Security Agency. (See footnote 23) After over 10 years of the public scrutiny, most experts are confident that DES is secure from virtually any adversary except a foreign government. (See footnote 24) DES is a private key cryptographic algorithm, which means that the confidentiality of the message, under normal conditions, is based on keeping the key secret between the sender and receiver of the message. (See footnote 25) DES specifies a cryptographic algorithm that converts plaintext to ciphertext using a 56-bit key. Encryption with the DES algorithm consists of 16 "rounds" of operations that mix the data and key together in a prescribed manner. The goal is to so completely scramble the data and key that every bit of ciphertext depends on every bit of the data plus every bit of the key. (See footnote 26)

In early 1993, the executive branch announced its policy to implement a new encryption device called "Clipper Chip," discussed in box A-1.

RSA–RSA is a patented public key encryption system that has been in use since 1978. It was invented at the Massachusetts Institute of Technology (MIT) by Ronald Rivest, Adi Shamir, and Leonard Adelman. These three inventors formed RSA Data Security, Inc. in 1982, and obtained an exclusive license for their invention from MIT, which owns the patent. The firm has developed proprietary software packages implementing the RSA cipher on personal computer networks. These packages, sold commercially, provide software-based communications safeguards, including message authentication, key management, and encryption. RSA relies on the difficulty of factoring large numbers to devise its encryption codes. Asymmetric cipher systems (like RSA) are more efficient than symmetric ones for digital signatures. (See footnote 27)

4.4.1 Personal Identification and User Verification

The purpose of user verification systems is to ensure that those accessing a computer or network are authorized to do so. Personal identification techniques are used to strengthen user verification by ensuring that the person actually is the authorized user. (See footnote 28) Authentication technology provides the basis for access control in computer systems. If the identity of a user can be correctly verified, legitimate users can be granted access to system resources. Conversely, those attempting to gain access without proper authorization can be denied. Once a user's identity is verified, access control techniques may be used to mediate the user's access to data.

The traditional method for authenticating users has been to provide them with a secret password, which must be used when requesting access to a particular system. However, authentication that relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons, including careless use and misuse–e.g., writing passwords on the terminal, under a desk blotter, etc. Where password-only authentication is not adequate for an application, a number of alternative methods can be used alone or in combination to increase the security of the authentication process. User verification systems generally involve a combination of criteria, such as something in an individual's possession, e.g., a coded card or token (token-based authentication), something the individual knows, e.g., a memorized password or personal identification number (password authentication), or some physical characteristic of the user, e.g., a fingerprint or voice pattern (biometric authentication). (See footnote 29)

Token-based authentication requires the system user to produce a physical token that the system can recognize as belonging to a legitimate user. These tokens typically contain information that is physically, magnetically, or electronically coded in a form that can be recognized by a host system. The most sophisticated tokens take the form of "smart cards," and contain one or more integrated circuits that can store and, in some cases, process information. (See footnote 30) Token-based systems reduce the threat from attackers who attempt to guess or steal passwords, because the attacker must either fabricate a counterfeit token or steal a valid token from a user and must know the user's password.

Biometric authentication relies on a unique physical characteristic to verify the identity of system users. Common biometric identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. The unique pattern that identifies a user is formed during an enrollment process, producing a template for that user. When a user wishes to authenticate access to the system, a physical measurement is made to obtain a current biometric pattern for the user. This pattern is compared to the enrollment template in order to verify the user's identity. Biometric authentication devices tend to cost more than password or token-based systems because the hardware required to capture and analyze biometric patterns is more complicated. However, biometrics provide a very high level of security because the authentication is directly related to a unique physical characteristic of the user that is difficult to counterfeit. At the same time, passwords, authentication tokens, and biometrics are subject to a variety of attacks.

New technologies and microelectronics, which are more difficult to counterfeit, have emerged to overcome these problems. These technologies have also enabled the merging of the identification criteria, so that one, two, or all the criteria can be used as needed. Microelectronics make the new user identification methods compact and portable. Electronic smart cards now carry prerecorded, usually encrypted access control information that must be compared with data that the proper authorized user is required to provide, such as a memorized personal identification number or biometric data like a fingerprint or retinal scan. (See footnote 31) Merging criteria allows authentication of the individual to his or her card or token and only then allows access to the protected computer or network. This can increase security since, for example, one's biometric characteristics cannot readily be given away, lost, or stolen. Biometrics permit automation of the personal identification/user verification process.

4.5 ACCESS CONTROL SOFTWARE AND AUDIT TRAILS

Once the identity of a user has a been verified, it is still necessary to ensure that he or she has access only to the resources and data that he or she is authorized to access. For host computers, these functions are performed by access control software. Records of users' accesses and online activities are maintained as audit trails by audit software. Access control methods include user identification codes, passwords, login controls, resource authorization, and authorization checking. These methods, as well as use of audit trails and journaling techniques, are discussed in box A-2.

4.6 COMPUTER ARCHITECTURE

The computer itself must be designed to facilitate good security, particularly for advanced security needs. For example, it should monitor its own activities in a reliable way, prevent users from gaining access to data they are not authorized to see, and be secure from sophisticated tampering or sabotage. However, while changes in computer architecture will gradually improve, particularly for larger computer users, more sophisticated architecture is not the primary need of the vast majority of current users outside of the national security community. Good user verification coupled with effective access controls, including controls on database management systems, are the more urgent needs for most users. (See footnote 32)

4.7 COMMUNICATIONS LINKAGES SAFEGUARDS

Computers are vulnerable to misuse through the ports that link them to telecommunication lines, as well as through taps on the lines themselves. As computers are linked through telecommunication systems, the problem of dial-up misuses by hackers may increase.

For purpose of this study, of particular interest in the area of medical information are port protection devices. (See footnote 33) One means of limiting misuse via dial-up lines has been dial-back port protection devices. Newer security modems are microprocessor-based devices that combine features of a modem with network security features, such as passwords, dial-back, and /or encryption, and offer added protection. For some computer applications, misuse via dial-up lines can be dramatically reduced by use of dial-back port protection devices used as a buffer between telecommunication lines and the computer. In addition to these dial-back systems, security modems can be used to protect data communication ports. These security modems are microprocessor-based devices that combine features of a modem with network security features, such as passwords, dial-back, and/or encryption. (See footnote 34)

4.8 APPENDIX A FOOTNOTES

1 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), pp. 42-43, 65-66, 83-85. This is a publication of the Committee on Improving the Patient Record, Division of Health Care Services. See also, Gretchen Murphy, "System and Data Protection," Aspects of the Computer-Based Patient Record, Marion J. Ball and Morris F. Collen, eds., (New York, NY: Springer-Verlog, 1992), p. 205.

2 See Gretchen Murphy, op. cit., footnote 1. For general definitions of security terms and concepts, see Dennis Longley, Michael Shain, William Caelli, Information Security: Dictionary of Concepts, Standards and Terms (New York, NY: Stockton Press, 1992).

3 Charles P. Pfleeger, Security in Computing (Englewood Cliffs, NJ: Prentice Hall, Inc. 1989), pp. 5-6.

4 National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy of Sciences,1991), p. 55. This is a publication of the System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications.

5 Ibid., p. 52.

6 See, Dennis Longley et al., op. cit., footnote 2, pp. 467-468.

7 National Research Council, op. cit., footnote 4, p. 50.

8 Ibid.

9 Ibid.

10 U.S. Department of Health and Human Services, Workgroup for Electronic Data Interchange, Report to the Secretary, July 1992, p. 29. However, the report later states that computer "hackers" have circumvented the security systems of a variety of computer systems; while access in some cases was limited to unauthorized "browsing" through database records, other instances of access have been accompanied by alteration or deletion of data or disruption of system operations.

11 See U.S. Congress, Office of Technology Assessment, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987); Robert H. Courtney, Jr., "Considerations of Information Security for Large Scale Digital Libraries," contractor report prepared for the Office of Technology Assessment, Mar. 27, 1993.

12 National Research Council, op. cit. footnote 4, pp. 50-51.

13 See Defending Secrets, op. cit., footnote 11, pp. 174-180. See also, Datapro Reports on Information Security, "Host File Encryption Software Overview," IS54-001-101, May 1992.

14 See generally, Defending Secrets, op. cit., footnote 11. See also, Datapro Reports on Information Security, "Host Security Software," IS50-140-103, November 1992, and generally, Dennis Longley et al., op. cit., footnote 2.

15 Encryption is an essential method for ensuring the three goals of computer security: confidentiality, integrity, and access. Encryption provides confidentiality for data. Encryption can also be used to achieve integrity, since data that cannot be read, generally cannot be changed. Encryption is important in establishment of secure communication protocols (a sequence of steps taken by two or more parties to accomplish some task) between users. Some of these protocols are implemented to ensure access to data. Defending Secrets, op. cit., footnote 11, pp. 54-63. See also, Datapro Reports, op. cit., footnote 13.

16 The words encode and decode, or encipher and decipher, are often used instead of the verbs encrypt and decrypt. A system for encryption and decryption is called a cryptosystem. Charles P. Pfleeger, op. cit., footnote 3, p. 23.

17 Charles P. Pfleeger, op. cit., footnote 3, p. 23.

18 NIST originally chose DSS, in part because of patent considerations. Some critics of the choice (including the company marketing the RSA system) have asserted that the RSA algorithm is superior and that NIST deliberately chose a weaker cipher. In late 1991, NIST's Computer Security and Privacy Advisory Board went on record as opposing adoption of the proposed DSS.

19 Defending Secrets, op. cit., footnote 11, p. 176.

20 Defending Secrets, op. cit., footnote 11, p. 180.

21 Defending Secrets, op. cit., footnote 11, pp. 54-55.

22 U.S. Department of Commerce, National Institute of Standards and Technology, NCSL Bulletin, Advising Users on Computer Systems Technology, June 1990.

23 Charles P. Pfleeger, op. cit., footnote 3, p. 107.

24 According to NIST, appropriate applications of DES include electronic funds transfer, privacy protection of personal information, personal authentication password protection, access control, etc., U.S. Department of Commerce, National Institute of Standards and Technology, NCSLBulletin, Advising Users on Computer Systems Technology, June 1990, pp. 1-2.

25 Defending Secrets, op. cit., footnote 11, p. 55.

26 Ibid.

27 Ibid., p. 63. See also, Datapro Reports on Information Security, "Microcomputer Encryption and Access Control: Technology Overview," IS31-001-125, April 1991, and Dennis Longley et. al., op. cit., footnote 2, pp. 165-171.

28 Defending Secrets, op. cit., footnote 11, p. 72. See also, Datapro Reports on Information Security, "Host Access Control Software Overview," IS52-001-103, July 1992.

29 Department of Commerce, National Institute of Standards and Technology, CSL Bulletin, Advising Users on Computer Systems Technology, November 1991.

30 For further discussion of use of smart card systems for health care information, see ch. 3.

31 CSL Bulletin, op. cit., footnote 29.

32 Defending Secrets, op. cit., footnote 11, pp. 88-89. See also, Dennis Longley et al., op. cit., footnote 2, p. 464.

33 Discussion of other communications linkage safeguards can be found in Defending Secrets, op. cit., footnote 11, pp. 89-92. See also, Dennis Longley et al., op. cit., footnote 2, p. 408.

34 Datapro Reports on Information Security "Protecting Information by Authentication and Encryption," IS50-140-103, June 1993.

MODEL CODES FOR PROTECTION OF HEALTH CARE INFORMATION

WORKSHOP PARTICIPANTS

Emerging Privacy Issues in the Computerization of Medical Records

Margaret Amatayakul
Associate Executive Director, Computer-based Patient Record Institute, Inc.

John Fanning
Senior Health Policy Advisor, Dept. of Health and Human Services

Diane Fulton
Legislative Policy Analyst, Blue Cross/Blue Shield

Elmer Gabrieli
President, Electronic Healthcare Records Research, Inc.

Janlori Goldman
Director, Privacy & Technology Project, American Civil Liberties Union

Holly Gwin (Chair)
General Counsel, Office of Technology Assessment

Thomas Marr
Senior Staff Investigator, Coldspring Harbor Laboratories

Randall Oates
Family Clinic, Springdale, Arkansas

George Trubow
Director, Center for Information Technology and Privacy Law, The John Marshall Law School

Designing Privacy in Computer Systems for Health Care Information

G. Octo Barnett
Director, Laboratory of Computer Science, Massachusetts General Hospital

Donna Dodson
Computer Specialist, National Institute of Standards and Technology

David Flaherty (Chair)
Professor History and Law, University of Western Ontario

Steven Brooks
Manager, Strategic Planning & Financial Analysis, Health Service Organization, Aetna Health Plans

W. Ed Hammond
Director, Division of Medical Informatics, Duke University Medical Center

Stuart Katzke
Chief, Computer Security Division, National Institute of Standards and Technology

Kevin McCurley
Senior Member of Technical Staff, Sandia National Laboratories

Gregory Pace
Senior Systems Advisor, Social Security Administration

Marc Rotenberg
Director, Washington Office, Computer Professionals for Social Responsibility

Harvey Schwartz
Senior Economist, Agency for Health Care Policy and Research

Willis Ware
Consultant, The Rand Corporation

Alan Westin
Professor of Public Law and Government, Columbia University

Michael Yesley
Coordinator, ELSI Program, Department of Energy

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provides by the workshop participants. The workshop participants do not, however, necessarily approve, disapprove, or endorse this background paper. OTA assumes full responsibility for the background paper and the accuracy of its contents.

PROJECT STAFF

Paula J. Bruening
Project Director

Ted Hammerman
Research Assistant (May-November 1992)

ADMINISTRATIVE STAFF

Liz Emanuel
Office Administrator

Michelle Smith
Secretary

Karolyn St. Clair
PC Specialist

John Andelin
Assistant Director, OTA, Science, Information, and Natural Resources Division

James W. Curlin
Program Manager, OTA, Telecommunication and Computing Technologies Program

REVIEWERS AND CONTRIBUTORS

Lois Alexander
Assistant to the Commissioner, Social Security Administration

Leslie Alexandre
Government Affairs Representative, EDS

Sheri Alpert
Consultant

Jerry Brager
Chairman and Chief Executive Officer, Physicians Computer Network, Inc.

Marjorie H. Carey
Assistant General Counsel, American Hospital Association

Stephan Chertoff
Director of Government Relations, PCS Health Systems, Inc.

Neil Day
President, MIB, Inc.

Charles Dougherty
Director, Center for Health Policy and Ethics, Creighton University

Denise Dougherty
Senior Associate, Office of Technology Assessment

Deirdre Duzor
Director, Division of Medicare Part A, Office of Legislation & Policy Health Care, Dept. of Health and Human Services

Hellen Gelband
Senior Associate, Office of Technology Assessment

David Hamilton
Director, Clinical Systems, Harvard Community Health Plan

Mary Alice Hanken
Medical Informatics Institute

Lawrence Hunter
Computer Scientist, National Library of Medicine

James Leglar
Department of Family Practice, University of Texas at San Antonio

Kathleen Lohr
Deputy Director, Division of Health Care Services, Institute of Medicine
Gerald Lore
Associate, Vice President and Director, Government Affairs, Hoffman-LaRoche
Robert McDonough
Senior Analyst, Office of Technology Assessment
Sean McLinden
GFN Healthcare, Inc.
Ben Miller
Chairman, CardTech/SecurTech
Elsbeth Monod
French Ministry of Social Affairs & Health
Jeff Neuberger
Brown Raysman & Milstein
Robyn Nishimi
Senior Associate, Office of Technology Assessment
Madison Powers
Associate Professor, Department of Philosophy, Georgetown University
Janet Sayles
Executive Director, Smart Card Industry Association
Jerome Seidenfeld
Government Affairs, American Medical Association
Nicole Simmons
Medicare Policy Analyst, Dept. of Health & Human Services
Dennis Steinauer
Computer Scientist, National Institute of Standards & Testing
Dana Theus
Industry Government Liasion for Information Technology, EDS
Joan Turek-Brezina
Chair, Task Force on Privacy of Private Sector Health Records, Dept. of Health & Human Services
Julia Wilson
Legislative Policy Analyst, Blue Cross/Blue Shield
Joan Winston
Senior Associate, Office of Technology Assessment

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the reviewers and contributors. The reviewers and contributors do not, however, necessarily approve, disapprove, or endorse this background paper OTA assumes full responsibility for the background paper and the accuracy of its contents.