Systems for Computerized Health Care Information

3

Implementation of a system for computerized medical information involves technological and nontechnologica1 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.

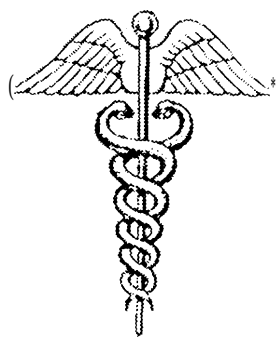
THE TECHNOLOGY OF COMPUTERIZED HEALTH CARE INFORMATION

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.[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.[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.[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 away 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 information such as those for medical research.[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 institutions No system can be made totally secure through technology.

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

---

[1] Gretchen Murphy, 'System and Data Protecting" *Aspects of the Computer Based Patient Record,* Marion J. Ball, Morns 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 physic@ 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.

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 networks, 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 networks, 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.[6] *The exten-*

[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' ofilces, medical schools, medical libraries, and universities; software and visualization technology for visualizing the human anatomy and analyzing x-ray, CAT Sea% 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.)

sive 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

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 seamers that read finger-prints, retinas, or speech patterns. These devices provide heightened security, but at higher cost.[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.[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 freed period of time will automatically revert to the password entry screen.[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.[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 deci-

---

[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.

sions about compliance with regulations about data. legal concerns, and ethical considerations regarding the transfer and release of information,

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,[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. *[12]

Definitions of what constitutes a smart card differ. Generally, a smart card encompasses off-linc 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 64 EEPROM (Electrically Erasable Programmable Read Only Memory)[13] reprogramming ble memory chip and microprocessor for internal power.[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 cards 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 funtions. 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.

SMART CARDS AS A MEANS OF INFORMATION STORAGE.[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

---

[11] The microprocessor is the component which distinguishes a smart card from cards designed 10 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.

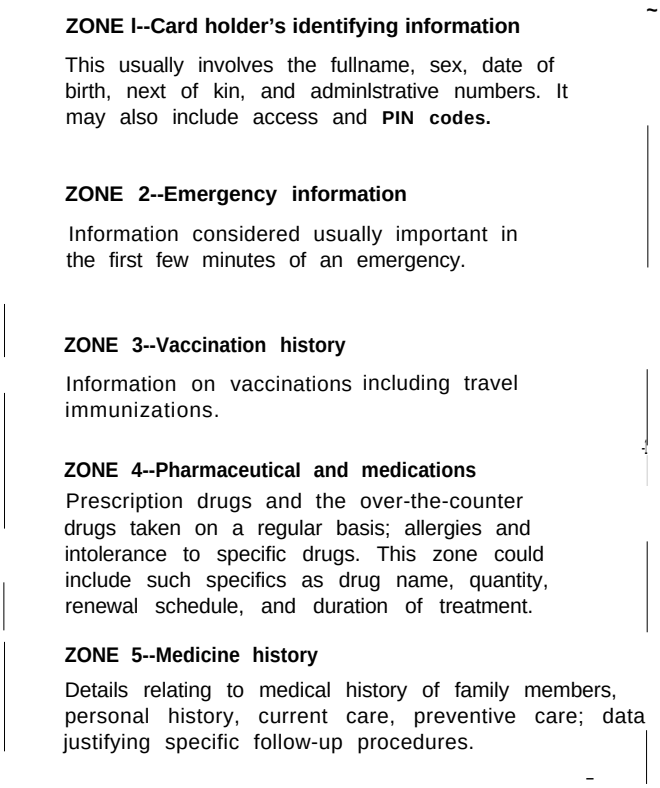
[12] Smart cards and access technologies are only one part of an overall computer security program. For a discussion of computer security measures, see app A

[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 curds 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 carder 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 GGAO6U1O, 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, L', 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.

Figure 3-I—Possible Applications of Smart Card Memory Zones for Medical Information



Illustrates how the health care information contained on the smart card maybe accessed and **used.**

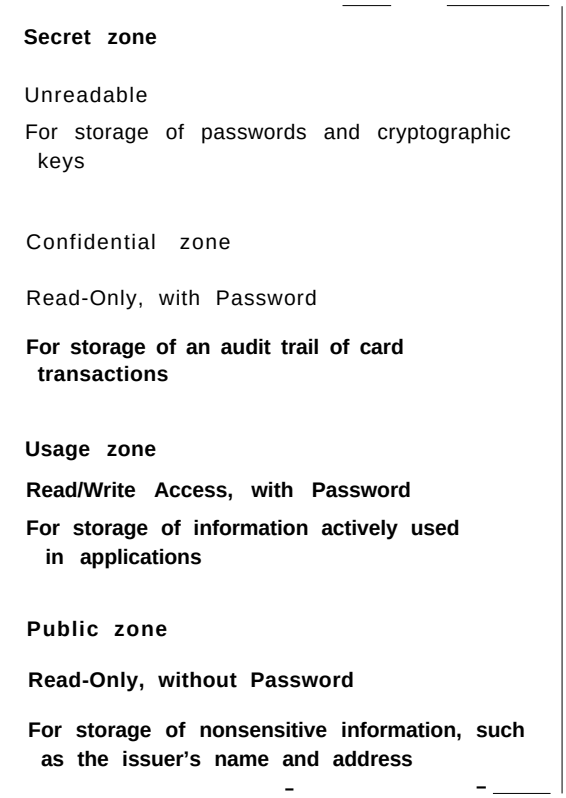
Zone 1: Identification information. All care providers would have access to this level. Only physicians, pharmacists and the issuing organization would be permitted to make entries.
Zone 2: Emergency information. All care providers would be authorized to read this zone. Only physicians would be authorized to make entries.
Zone 3: Vaccination information. All providers with the exception of ambulance personnel would be authorized to read this zone, but only physicians and nurses could make entries.
Zone 4: Medication information. Only physicians and pharmacists would be permitted to read or write in this zone.
Zone 5: Medicine history. Only physicians would be permitted to read or write in this zone.

SOURCE: Simon Davies, *Big Brother: Australia's Growing Web of Surveillance* **(Australia: Simon and Schuster, 1992), and Office of Technology Assessment, 1993.**

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

Figure 3-2—Possible Smart Card Memory Zones



This figure illustrates a possible smart card memory divided into four zones: a secret zone, a confidential zone, a usage zone, and a public zone. A secret zone could be used for storage of information that can be used only by the microprocessor itself. Passwords, cryptographic keys, the card bearer's digitized fingerprint, or any other information which shouid never be readable outside of the smart card could be stored in this zone.

SOURCE: Martha E. Haykin and Robert B.J. Warnar, "Smart Card Technology: New Methods for Computer Access Control," NIST Special Publication 500-157, September 1988, p. 25.

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.

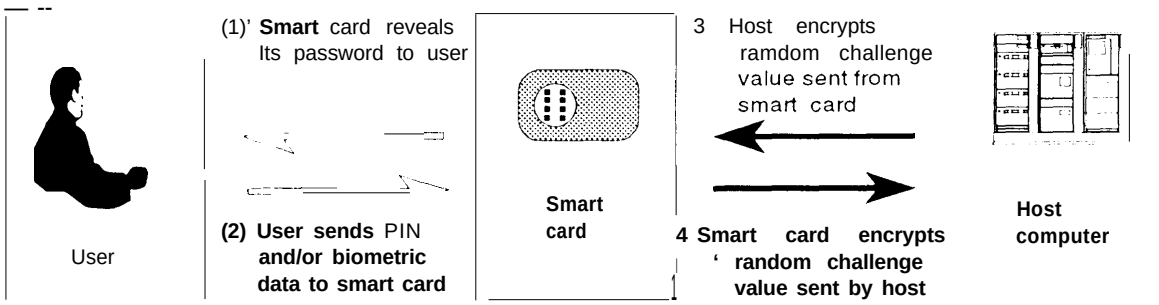
Crucial secret information can be maintained in separate protected memory locations through the use of the smart card's memory zones. It may also be possible to produce a smart card that would ensure that the entire secret zone will be destroyed if any attempt is made to access the data in that zone; 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.)

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 terrninal (see figure 3-3). A smart card is intended to remain in

Figure 3-3-A System of Authentication Using Smart Cards



NOTE: This figure illustrates the use of a smart card in a process of authentication between a user and a host. Though a system of authentication using smart cards can be very intricate, it does not demand that the user perform any complicated operations. The commands needed to initiate and carry out the process are stored within the smart card. Thus, the user **only needs to memorize one PIN and be able to recognize the smart card's password.**

SOURCE: Martha E. Haykin and Robert B.J. Warnar, *Smart Card Technology:NewMethods of Computer Access Control,* **NIST Special Publication 500-157, September 1988, p. 23.**

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.

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.[16] me **frequent 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 nformation.[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 non government organization) which will maintain a network of back-up centers throughout the country. This electronic record will have several levels

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.

Box 3-A-The French System: A Smart Card Approach

The French Social Security System and the Health Insurance Scheme

The French Social Security system was established shortly after World War II and was designed to work on the basis of mutual cooperation between all beneficiaries. The compulsory Health Insurance scheme is administered by employers and representatives of workers subscribing to the system. The Social Security system, which is financially independent from the State, draws its resources from contributions paid by people insured and their employers. These contributions are calculated according to earnings.

The Health Insurance branch of the Social Security system performs two main roles:

1. It reimburses most health charges incurred by French workers and their families. Presently someone requiring medical treatment can expect to have about 75 percent of his ambulatory care bills reimbursed by Social Security.
2. The Social Security System provides a guaranteed income for people unemployed for medical reasons.

in addition to belonging to the statutory, compulsory Social Securit y system, the French are often covered either by complementary health insurance contracts negotiated by their employers with nonprofit mutual insurance companies, or by contracts with private health insurance companies. This enables the patient, once Social Security has reimbursed him or her about 75 percent, to recover part or all of t he remaining 25 percent. Approximately 80 percent of the population has supplementary private or nonprofit health insurance. Although there are only three major compulsory health insurance schemes in France, there are over 10 thousand complementary Insurance organizations.

Growth in Health Expenditures and Information Flows

Transfer of information and communication between all the public and private health professionals and institutions in this sector is increasing rapidly. The exchange of medical and administrative data between patients and the Social Security Organization, nonprofit insurance companies (known as mutuelles) and private insurance companies shows a similartrend. The Health Insurance branch of the Social Security System in 1989 processed 760 million paper health care reimbursement claims.

in its efforts to reduce the cost of health care, the government is attempting at the same time to preserve the fundamental principles of the French health service: free choice of health services for patients; free choice on the part of doctors as to methods; conditions and areas to establish medical practice; and respect for the confidentiality of medical information and the protection of individual rights. The Health Professional Card (discussed below) was designed to assist in this effort.

Card Systems

SESA/WVITALE PROJECT of the Social Security Organization

Among experiments involving the use of smart cards, the Social Security Organization's SESAMMTALE is a system aimed at the substitution of the Social Security insurance paper card (45 m i H ion are issued every year) as well as the 800 m ill ionreimbursement claim forms processed per year, by a m icrochip card called VITALE, a "portable family administrative file." Ail paper transactions will be replaced by electronic information transfers. The essential purpose of the SESAM/VITALE project is to improve the quality of adminstrative services and to reduce costs. As of 1992,300,000 cards have been issued in the SESAM/VITALE Project.

(continuedon next page)

Box 3-A–The French System: A Smart Card Approach-Continued

MUUTUSANTE CARD of the *Mutuelle Medicale et Chimrgicale des Alpes*

Mutusante is issued by the Alpes Surgery and Medical Mutuelle in Digne. In 1987 the Mutuelle decided to launch a smart card project with the following objectives in mind:

- **simplifying and reducing administrative procedures;**
- **replacing financial paper transactions by electronic transfers between the different organizations; and**
- **allowing prepaid health care services for drugs and laboratory work.**

The card contains personal identification, identification of all members of the family and their insurance coverage, the rights and dates of validation. By the end of 1992,50,000 cards were distributed in this program.

***Carte Sante of the Federation des Mutuelles de France* (SMS)**

The aim of this project, now being implemented in various sites throughout France, is to offer new services to members of the Mutuelle and to establish a new partnership with health professionals in offering new services, particularly financial ones. In this program, 250,000 cards have been issued. The card contains

1. **Social Security and Mutuelle rights;**
2. **bank references to allow for deferred payment;**
3. **an emergency zone with emergency data, permanent data such as blood group and missing organs, and variable data such as pregnancy, special treatments, etc;**
4. **a surveillance zone listing illnesses and periodic examinations, their dates and locations, regular cheek-ups; and**
5. **a preventive zone including the work environment with its specific risks and genetic factors.**

Updating of the card is possible at the doctor's office or at any branch of the Mutuelle.

SANTAL *CARD of the Centre Hospitalier de Saint-Nazaire*

The Santal system was first tested in 1987 in the Saint Nazaire area of France and was developed in close collaboration with members of the medical profession. Thirt y-two thousand patients as well as hundreds of health professionals and employees are now involved. Four public hospitals, 4 private clinics, and 11 laboratories and health insurance companies are also participating in the project.

The aims of the project are to facilitate reception of patients at medical facilities, to provide easier communication between hospital services, and to optimize use of hospital and medical resources.

The Santal card includes an administrative section concerning the personal identification and health insurance affiliation, the names of the doctor and of persons to be alerted in case of an emergency; a medical segment used as an alert to significant surgeries, in-patient hospitalizations or out-patient diagnoses, drug treatments, previous hospital stays, date of admissions, etc.; and data concerning blood groups, nurses' files, and prescription information.

DIALYBRE *CARD of the Fondation de L'Avenir*

Dialybre is a project supported by the French mutuality organizations, with the purpose of increasing patient autonomy and mobility, and keeping medical information current.

The early pilot study was launched in 1988. The system consists of a smart card, used as a hand portable, minimum medical file given to every patient with terminal renal failure treated by hemodialysis. Patients undergoing hemodialysis are free to travel from center to center for treatment. The Dialybre

Card carries the minimum data records concerning the care given to the patient. By the end of 1992, 6,000 cards were in use in this program.

CARTE DU PROFESSIONNEL DE SANTE (Health Professional Card)

The French see the use of a "Health Professional Card" as the key to promoting coherent communication and security between all the different health information systems (patient Smart Card systems as well as traditional medical information system), while at the same time respecting the autonomy of various participants in the system in making management decisions.

The Health Professional Card is a smart card designed to give nationwide identification of health care professionals to be used as a single access key to all the medical and social securit y dat a systems. It is issued in partnership between the Ministry of Health and Social Securit y, professional unions and all sector's organizations. It has been conceived by representatives of the professions doctors, pharmacists, nurses, dentists, midwives, etc, and will be issued to France's health professionals.

The Health Professional Card is a portable data support tool permitting the holder to identify himself or hersetf, to state his or her professional qualifications, to read and/or write medical information f rom medical files or health cards according to their status and qualif ication within the health care system, and to sign electronically the medical information put into the patient card or database. It is seen by some as a sort of "box" of safety measures for the broader smart card system for health care, providing a source for identification, authentication, certification, electronic signature, and encryption. The Health Professional Card, it is believed, allows for integration of a variety of computerized information sources only by appropriate persons. At the same time, these databases can remain decentralized, which many believe is imperative to maintaining the confidentialit y of the data contained in them. Approximately 1.3 million health professionals are expected to be issued cards.

While planning for the implementation of this technology, the French Ministry of Social Affairs and Health has also been working with its partners to determine laws and regulations to permit the implementation and use of this technology. The challenge is to balance legal, institutional, technical, administrative and social demands to provide computerized health services.

SOURCE: Elsbeth Monod, Mission Carte Communication Sante, International Relations, French Ministry of Social Affairs and Health, 1992.

of security restriction which will control who will have access to what part of each encounter.[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,[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

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.

Box 3-B-international Examples of Health Care Applications for Smart Cards

Since the mid-1980s, approximately 100 pilot projects using smart cards for medical purposes have been initiated internationally.

Applications for smart cards in health care can be classified in two major categories: cards with administrative data and cards with clinical data. International pilot projects have tested various applications.

Identification and social securityc ard **replaces an existing paper insurance card for identification of the patient and his or her claim.**

Health pass: replaces an existing paper health card for patients who need intensive care in a particular phase of their lives (mother-child pass, senior citizen pass, health examination pass).

Genera/ patient card: **a patient health card on which the patient's medical record is stored; the primary aim is to improve the information flow within the entire health service.**

Blood type card: replaces an existing paper blood group card.

Emergencycard replaces an existing paper identification card of an accident patient and provides the immediate availability of emergency data.

Work or sports medical card: **replaces and introduces a card for a particular group of people who are under permanent medical supervision or who are exposed to special risks.**

Risk *group card:* introduces a specialized patient card for patients with chronic pathologies requiring long-term treatment or medication.

Labartory pharmacy card: **a card facilitating communication between the prescribing doctor and the laboratory or pharmacist, as a means of conveying accurate information.**

Payment or accounting card that **rationalizes accounting and cost refunding and facilitates finanicial transactions.**

SOURCE: Claudia Wild and Walter Peissl, "Patient Cards: An Assessment of a New Information techology in Health Care," *IT in Medicine,* **Project Apraisal** *vol. 7, No. 2,* **June 1992, pp. 68-74.**

proposed as one solution to the need to contain costs, streamline paperwork, and increase availability of health care services.[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 excep-

m Major proposals before the 102d Cougress 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.

tion, probably, of emergency information) .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.[22]

However, critics of such a system cite shortcomings of the card's ability to protect patient privacy in medical information. Concerns have been raised about patient compliance with carrying the card .[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).[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 carry ing.[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 .26 Concerns remain, also, about security of information at the host.[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.[28] From the standpoint of health care research, questions remain to what extent this system would hinder epidemiologists' efforts to examine the course of diseases

---

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.

through access to medical records.[29] Still others indicate their uneasiness with a system of identifi cation 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.[30]

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 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 place of birth, or place of issuance of the number.[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.[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.[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.[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 informa-

---

2$' 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 bean "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 use 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.

tion held both by the government and private companies,[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.[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, finacial, 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*[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. ''[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.[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.[40]

---

35 U.S. Department of Health, Education, and Welfare, The Secretary 's Advisory Committee on Automated Personal Data Systems, Records, *Computerland 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: Quadrangle 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 impersonal information, whether health care information or otherwise. Sean McLinden, op.cit., footnote 28.

The experience of Ontario, Canada with unique patient identifiers in delivering health care benefits is useful.[41] All Canadian provinces have some type of health identifacation 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, lifetime, 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.[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. '[43]

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.*[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 transmission 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.[45] Currently, the terms used to describe the

---

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, ''~vacy, 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.

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.[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.[47] Although there is general agreement 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 computerized 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 secondary 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

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.

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. ''[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.[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.[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 .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-

---

48 The American Health Information h@ nagement Association defines ''medical information' as arty 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 withio 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. 'I'he 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, ''hgal 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, ''prescrib~g 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.

Box 3-C-Standards Development Efforts

Among the groups developing standards for health care information systems in the areas of communication protocols and the characteristics of information collection and use are the Institute of Electrical and Electronics Engineers (IEEE), the American Society for Testing Materials (ASTM), the International Standards Organization (ISO), and Health Level 7 (HL7), the only standard currently being implemented by vendors.

To facilitate the establishment of such standards, the American National Standards Institute has established a Healthcare Informatics Standard Planning Panel (HISPP). Its charter is to set forth standards for:

1. **health care models and electronic health care records;**
2. **the interchange of health care data, images, sounds and signals within and between organizations/practices;**
3. **health care codes and terminology;**
4. **the communication with diagnostic instruments and health care devices;**
5. **the representation and communication of health care protocols, knowledge, and statistical databases;**
6. **privacy, confidentiality and security of medical information; and**
7. **additional areas of concern or interest with regard to health care informational**

The planning panel coordinates the work of the standards groups for health care data interchange and other relevant standards groups toward development of a unified set of standards that are compatible in International Standards Organization (ISO) as well as non-ISO communications environments.

The ANSI HISPP coordinates organizations and committees that develop standards, but does not write standards *or* make technical determinations, leaving this function to the accredited standards development organizations and committees. Those interested in the development of these standards are encouraged to enter into this discussion, thus fostering cooperation and coordination.

Voting membership in the ANSI HISPP consists of private companies, government agencies, individual experts, and other organizations. The membership is classified by interest groups, e.g., users, producers, professional and trade associations, government agencies, and standards developers. ANSI HISPP acts on the basis of a majorit y vote of the full voting membership, either at a meeting with a quorum present, or by letter ballot.

[1] **American National Standards Institute, Healthcare Informatics Standards Planning Panel (HISPP), "Charter Statement," Revised September 1992.**

SOURCE: The American Health Information Management Association, 1992.

know" with the privacy interests of the patient.[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.*

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

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

to third parties.[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.[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.[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.[56]

The general rule is that the owner of the paper on which the medical record is maintained is the ''owner' of the record.[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. However, 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 .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

---

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 cd., 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 Me&~ Records: A Proposal fora 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 treating a patient are primarily for the physician's own use and constitute his personal properly. " 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.

community. The use of the medical record as a general source of information for decisions and control in nontrementn 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 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 .59

In spite of the requests made of them to authorize disclosure of medical information for medical and nonmedicaI purposes, patients traditionlly have been unable to inspect their own records, and laws governing patients' access to records are not universal or uniform.[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.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.[62] However, this approach to the patient record arguably conflicts with patient rights and autonomy .63

> Traditionally, the medical rationale for withholding 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,[64]

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.

61 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 "event hough 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 generat 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.

While the majority of States grant individuals a legal right to see and copy their medical records by statute, regulation or judicial decision,[65] laws regulating patient access to health records are not uniform or even universal. Federal regulations for substance abuse programs,[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 cirumstances.[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. ''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.[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

---

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.

precludes access, and where minors are governed by legal constraints.[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 understanding 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.[72] Some commentators suggest that patient consent forms for disclosure of information should be required to contain a checklist detailing what information can be released, to whom it may be sent, for what purpose it maybe used, and for what period of time.[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 .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.[75] Yet others recommend at minimum "a policy decision not to honor statements of unrestricted scope. ' '[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.*

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 reasonable use of certain medical information by the system for prescribed purposes. Once that reasonable 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.

---

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.