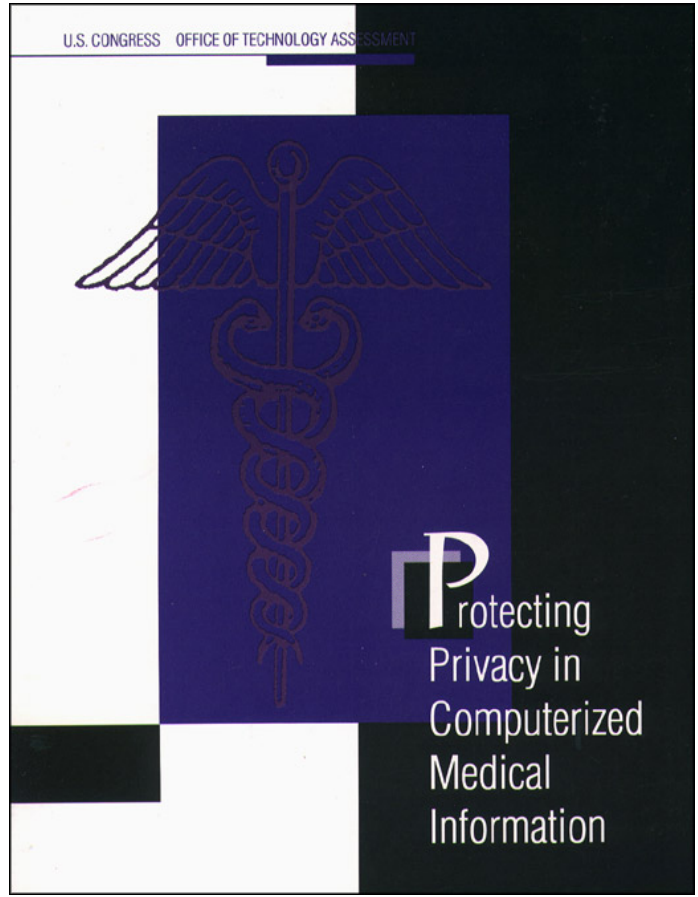
Protecting Privacy in Computerized Medical Information

September 1993

OTA-TCT-576
NTIS order #PB94-107646



Recommended Citation:
U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information, OTA-TCT-576* (Washington, DC: U.S. Government Printing Office, September 1993).

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328
ISBN 0-16-042074-1

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 efficentefllcient 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

Workshop Participants

Emerging Privacy Issues in the Computerization of Medical Records

Margret 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 Laboratones

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 Helth 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 A dministration

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 provided 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**

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

–
May-November 1992

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 Goverment 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 accuarcy of contents.

Contents

1 Introduction, Summary, and Options 1

Background and Study Approach 1
The Need for Privacy in Health Care Information 5
The Computerization of Medical Records 6
Protection for Privacy in Health Care Information 12
Special Policy Problems Raised by Computerization 16
Models for Protection of Computerized Medical Information 18
Congressional Options 19

2 The Right to Privacy in Health Care Information 23

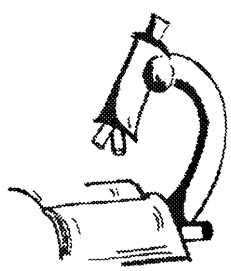
Why is Privacy in Health Care Information Important? 26
Unregulated Computerization and Marketing of Health Care Information 30
Potential for Increased Demands for Computerized Information 31
Issues Raised by Computerization 36
Right to Privacy in Health Care Information 38
Federal Law Protecting Privacy in Medical Records 41
Sources of the Confidentiality Obligation-State Common Law 42
Sources of Confidentiality Obligation—State Statutes 43
Inadequacy of Existing Protection Scheme and the Need for Federal Legislation 44

3 Systems for Computerized Health Care Information 51

The Technology of Computerized Health Care Information 51
The Unique Patient Identifier 64







Standards for Computerized Medical Information 66
Informed Consent to Disclosure of Information 69

4 Designing Protection for Computerized Health Care Information 75

Fair Information Practices and the Privacy Act 77
Features of Health Care Privacy Legislation 79

APPENDIXES

A Selected Topics in Computer Security 89

B Model Codes for Protection of Health Care Information 101

INDEX 153

Introduction, Summary, and Options

1

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

BACKGROUND AND STUDY APPROACH

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

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

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

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

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

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

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

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

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

What Is Health Care Information?

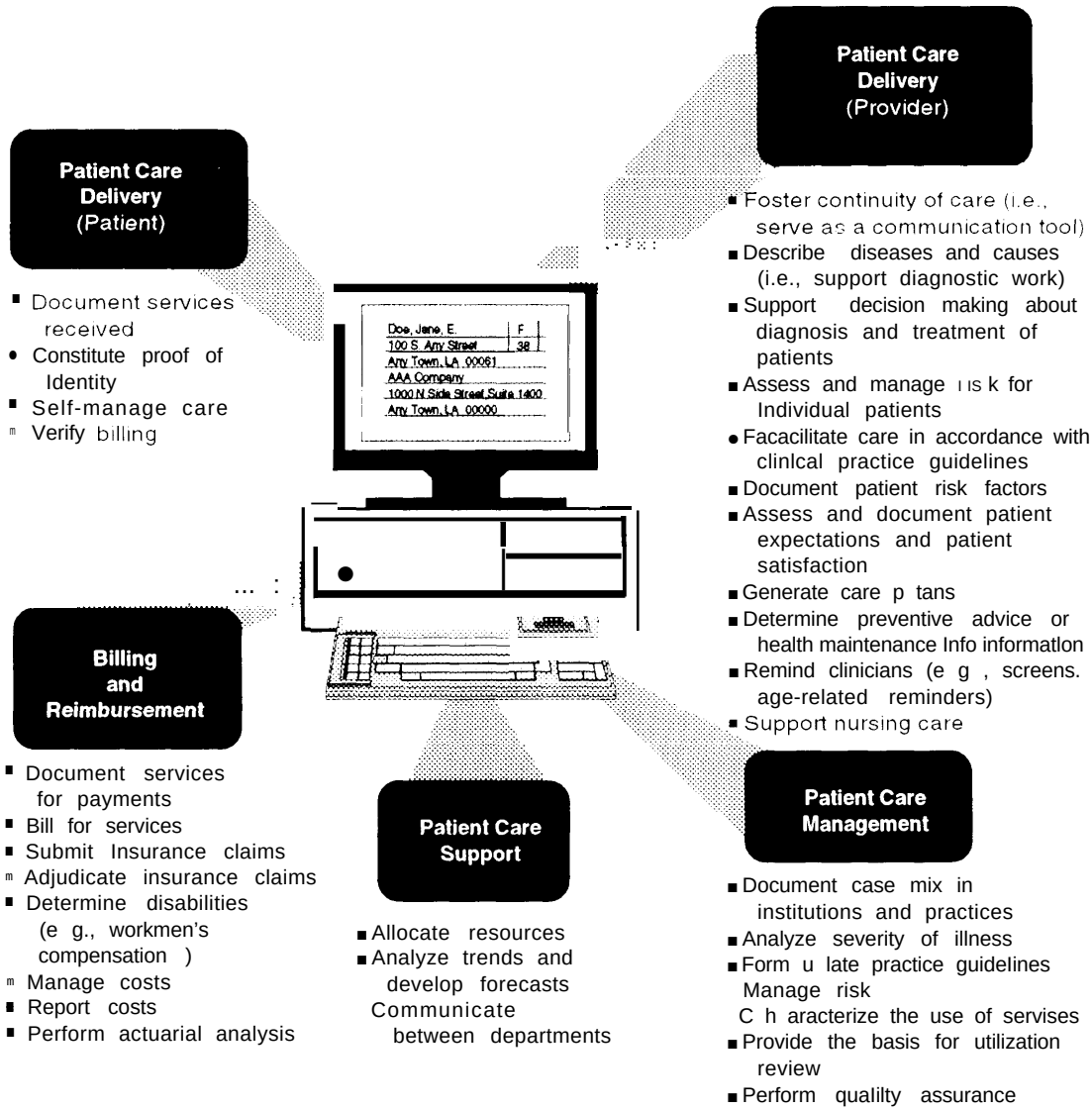
The Institute of Medicine report, *The Computer-Based Patient Record: An Essential Technology for Health Care*[3] (hereinafter referred to as the "IOM report") recommends that health care professionals and organizations should adopt the computer-based patient record for use in online systems as the standard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

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

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

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

Figure I-I—Primary Uses of Patient Records

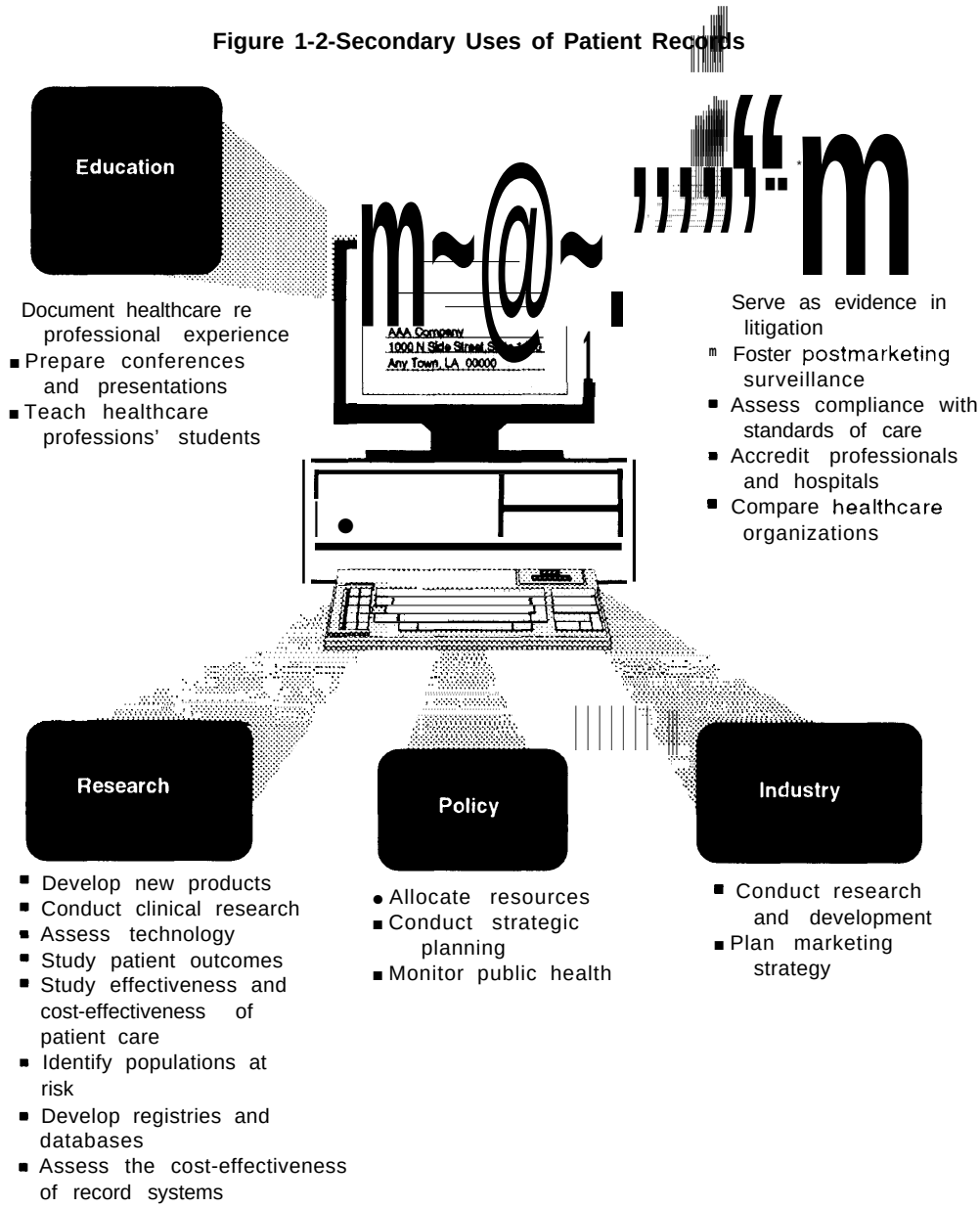


SOURCE: American Health Information Management Association (AHIMA), 1993, based on information contained in Institute of Medicine, The Computer-Based Patient *Record:An Essential Technology for Health Care,* Richard J. Dick and Elaine B, Steen, eds., (Washington, DC: National Academy Press, 1991).

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

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

Figure 1-2-Secondary Uses of Patient Records



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

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

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

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

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

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

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

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

THE NEED FOR PRIVACY IN HEALTH CARE INFORMATION

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



A medical information computer searching center.

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

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

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

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

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

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

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

THE COMPUTERIZATION OF MEDICAL RECORDS

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

(Continued on next page)

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

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

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

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

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

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

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

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

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

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

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

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

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

10 Ibid.

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

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

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

---

8 Ibid.

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

10 Ibid.

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

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

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

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

11 Ibid., p. 45.

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


JOHN STEY, UNIVERSITY OF CONNECTICUT HEALTH CENTER

A health care practitioner searches an online medical research database,

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

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

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

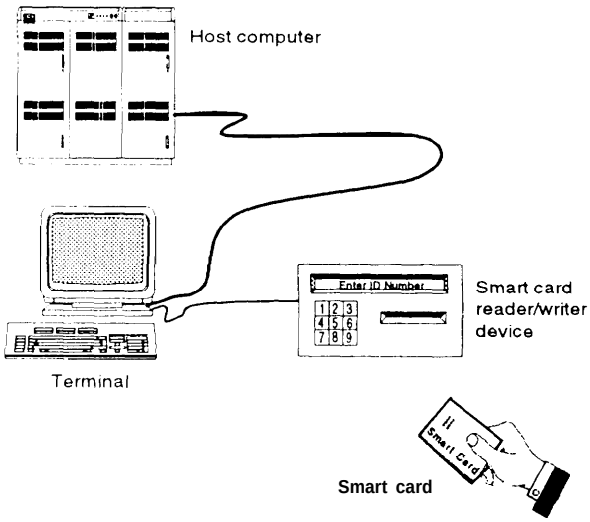
---

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

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

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

Figure 1-3-Generalized Smart Card System



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

Computerization of Health Care Information by Private Companies

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

Security and Confidentiality Measures

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

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

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

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

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

Online Systems

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

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

Smart Cards

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

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

PROTECTION FOR PRIVACY IN HEALTH CARE INFORMATION

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

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

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

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

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

SOURCE: Office of Technology Assessment, 1993.

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

Ethical Sources

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

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

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

Legal Origins

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

FEDERAL LAW

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

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

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

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

Health and Human Services, except as prescribed by regulation.

STATE LAWS AND REGULATIONS

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

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

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

1 The Effect of Computers on the Question of Privacy

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

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

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

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

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

SPECIAL POLICY PROBLEMS RAISED BY COMPUTERIZATION

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

1 The Unique Patient Identifier

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

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

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

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

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

Informed Patient Consent to Information Disclosure

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

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

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

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

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

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

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

1 Standards

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

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

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

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

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

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

MODELS FOR PROTECTION OF COMPUTERIZED MEDICAL INFORMATION

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

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

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

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

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

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

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

CONGRESSIONAL OPTIONS

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

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

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

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

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

located in different States and operating under different State laws.

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

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

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

Such legislation would:

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

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

Option 2, Monitor standard setting

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

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

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

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

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

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

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

---

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

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

The Right to Privacy in Health Care Information 2

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.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.[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:



[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.

- 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.[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.[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 determination; 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 processing of insurance and managed-care administrative transactions, such as claims, eligibility checks, and coordinating benefits, could streamline payers' 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.[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. 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.

---

[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.

The Report of the Work Group on Computerization of Patient Records to the Secretary of the U.S. Department of Health & Human Services[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[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

[7] U.S. Department of Health and Human Services, Work Group on Computerization of Patient Records, Report to the Secretary, ''lbWard 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.

advance. California's Privacy Rights Clearinghouse, the first privacy hotline in the Nation, logged more than 5,400 calls within 3 months of it inception in November 1992.[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.[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.[11]

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

---

[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.

Box 2-A—instances of Health Care Information Abuse United States

- While researching the life of a well known member of the film industry, a journalist entered a New York hospital disguised as a physician. The journalist obtained the actress' medical record and published that the actress had been treated for asexually transmitted disease.
- While a prominent Washington politician was under consideration for a Federal Government post, researchers reviewed his personal data and found that 26 years earlier he had been admitted into a mental institution. Although details of his treatment were unclear, on the basis of the information he was eliminated from consideration for the post.
- A Colorado medical student provided medical records to attorneys practicing malpractice law, copying them in the medical records department at night and selling them to in-State and out-of-State attorneys for $50.00 each.

SOURCE: Comments of Peter Waegemann, Executive Director, Medical Records Institute, to the Conference on Health Records: Social Needs and Personal Privacy, Washington DC, Feb. 11-12, 1993.

- A researcher conducted two studies on tobacco and cancer and assured his research subjects that the information they provided would remain confidential. In a lawsuit not involving the researcher or the two institutions where the information is stored, American Tobacco and two other companies compelled the researcher by subpoena to provide the data. A court held him in contempt for failing to comply, though it noted that it would take more than 1000 hours to delete data identifying the study subjects.[1]
- In an article on emergency health care technologies, a local newspaper published details of B. J.R.'s wife's fatal illness. Despite B.J.R.'s distress, a court ruled that the newspaper was free from liability.[2]
- A physician was tested for the AIDS virus as part of a survey of health-care workers. Although the physician was promised conf identicality, the researcher disclosed the fact of her positive test result to her employer, the county hospital. The physician learned the results of her AIDS test through her employer.[3]
- An insurance company discovered that one of its agents had AIDS and terminated him without the 30-day notice required in its contract. The man died before recovering $16,000 in back pay through arbitration.[4]
- On the basis of parents' objections to reported curious remarks made by a school bus driver while driving children on his route, the school superintendent investigated the complaints and reported that as long as the driver followed his medical regimen there was little likelihood t hat his disorder would interfere with his work. The parents insisted on seeing complete medical reports on the driver, and in 1986 the State Supreme Court ruled that they were entitled to them.[5]
- A physician under contract with R. B,'s company discussed the individual's health condition with managers, in apparent violation of the company's rules on the confidentiality of employee inform ation.[6]

1 *Mount Sinai School of Medicine* v. *American Tobacco* CO., 866 F. 2d 552 (2d Cir. 1989).

2 *The Morning Call*, Allentown PA, Nov. 19, 1982, *Privacy Journal*, victims file.

3 AssociatedPress story dated Jan. 2, 1990, *New* York *Times*, Jan. 24, 1990, p. B-3.

4 *Privacy Journal*, September 1987, P. 5.

5 *Morgantown Dominion Post*, Morgantown, WV, Nov. 13, 1989, p, 1; *Privacy Journal*, victims file.

6 *Bratt* v. *IBM Corp.*, 785 F. 2d 352 (1986); *Privacy Journal*, May 1986, p. 6.

SOURCE: Robert Ellis Smith, wfth Eric Siegel, *War Stories: Accounts of Persons Vicitmized by Invasions of Privacy*, July 1990.

Box 2-B-Investigation of Information Brokering--An International View

The Krever Commission

On Sept. *30,1930,* the Royal Commission of Inquiry Into the Confidentlaiity of Health Records in Ontario, Canada headed by Mr. Justice Horace Krever (The KreverCommk@on), submitted its report about abuse of confidential health information. That report dealt with the breaches of privacy in information maintained in both paper and computer record keeping systems. The KreverCommission found that the acquisition of medical information by private investigators without patient consent and through false pretenses was widespread.1 During a 14-mnonth period, the Krever Commission heard from over 5000 witnesses, including private investigative firms, insurance companies, hospitals and others. For the years 1976 and 1977, the Krever Commission found that there were hundreds of attempts made in Ontario to acquire medical information without consent from hospitals and physicians, and that over half of the attempts were successful.

As a result of the Krever Commission's inquest, several investigative firms went out of*business. So* many insurance *companies* were found to have been using medical information obtained under false pretenses that the Insurance Bureau of Canada made a general admission to the Royal Commission that is members had gathered medical information through various soureswithoutthe authorization of the patient.

The Independent Commission Agaist Corruption of New South Wales

in 1992, the Independent Commission Against Corruption of New South Wales released its Report on unauthorized government Information. Accoording to the report, Its Investigation revealed a massive Illicit trade in government information. Standard practice in this trade was to buy and sell government information, In some casses on a very large scale, for purposes of locating debtors and preparing for civil and criminal litigaation. The most common sorces for information were driver's license and motor vechile registration, police records, government departments and agencies, and, in spite oforimlnal sanotions provided by the Social Secrurity Ad of New South Wales, information from the Department of Social Security. Principal participants include public officials of New South Wales, who sold information, insurance companies, banks and flnancial institutions that provided a market information and private investigators who act as Information brokers and retailers.[2]

---

1 For an explanation of the methods used by the Krever Commission to uncover these abuses, see Federal Privacy of Medical *Information* Act, *S.* Rept. 96-832, Part 1, 96th Cong., *Mar.* 19,1080, pp. 24-28.

2 "Report on Unauthorized Release of Government Information," Publication of The Independent Commission Against Corruption, vol. 1, August 1992, Ian Temby, Commissioner.

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

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.[12] Staff comments about the patient's character or demeaner 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

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

Box 2-C-=Investigations of Information Brokering-The United States

The U.S. Social Security Admlnistratlon

As part of its system modernization effort, the Social Security Administration (SSA) converted many of its files to online databases. As a result of these efforts, claims processing was vastly streamlined. While the SSA took steps to safeguard the records in this database, the new ease of access brought with it new threats to the confidentiality of records, a fact revealed in an investigation of suspected misconduct by SSA employees. The Office of the Inspector General (OIG) investigated 200 allegations cd illegal disclosure of confidential information by Social Security Administration employees.

The computerization of the files making the Mor making immediately accessible and vastly more systematized than paper files, coupled with the personal nature of the information housed in SSA records, made the records an attractive target for individuals attempting to obtain or authenticate information. The OIG testified before the Subcommittee on Social Security and Family Policy that there has been an expansion in the number of "information brokers" who attempt to obtain, buy and sell SSA information to private companies, for their use in boating people or making decisions on hiring, firing, using or lending. As the demand for the information grows, brokers turn to increasingly illegal methods.

In a case involving Nationwide Electronic Tracking (NET), a florida based firm that promised "instant access" to "confidential data . . .24 hours a day, 7 days a week" 23 individuals, including private investigators, department employees, and law enforcement officers, were indicted by Federal grand juries for buying *and* selling confidential information held in government computers. The information released included SSA earnings information, Social Security numbers, full names, dates of birth, names of parents, names of all current and past employers, salary information, and other nonpublic information. The investigation revealed that the government employees were allegedly bribed for access to the information, which was then sold.

The OIG identified three methods used by information brokers to obtain SSA information. First, the broker entered into a "contract" with one or more SSA employees, who sold earnings histories to the brokers for about $25 a piece. The brokers marked up the price to $300 or more. Brokers tended to set a fee schedule, depending on the type of information requested and how quickly it was needed. Second, brokers went through an entity that legitimately contracted with SSA to obtain earnings record information. These entities included private investigators, insurance companies, law enforcement personnel, attorneys, credit unions, and employment agencies. Theo ontract holderfurnished a forged Social Security number release form to the SSA office of central records operation, which then supplied the information within 6 weeks. A third scheme was "pretesting." This method, generally used by private investigators, involved calling an SSA office, claiming to be an SSA employee from another office where the computers were down. The employee was requested to obtain the information and read it over the phone. The investigator then wrote down the information and passed it to his client.

SOURCE: Statement of Larry D. Morey, Deputy Inspector General for Investigations, Department of Health and Human Services, In Hearings before the Subcommittee on Social Security and Family Policy, Feb, 28,1992, S. Hearing 102-679, pp. 62-87.

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.[13] Medical conditions have served as the basis for

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

discriminatory practices, making it difficult to participate in these activities.[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.[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. [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 .17

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,[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

---

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 freed 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 discrumination 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.

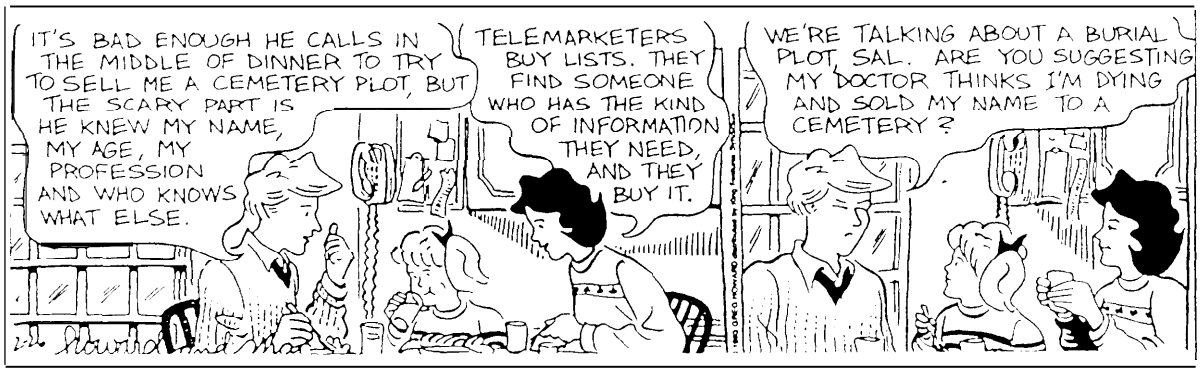
15 For example, is information on chronic health conditions, when used to determine whether or not to employ specific individuals, sensitive? Different persons will also vary in their perceptions of what is sensitive, and thus what constitutes an invasion of privacy may vary from person to person. Joan 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 Commissio, *Personal Privacy in an Information Society* (Washington DC: U.S. Government fin@ 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.

SALLY FORTH HOWARD & MACINTOSH



HOWARD & MACINTOSH, KING FEATURES SYNDICATE

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.[19] The businesses involved in these ventures operate under no regulatory guidelines regarding security measures, employee practices, or licensing requirements.

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.[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 dollars for health services .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.[22]

Demands for information come not only from review bodies, third-party payers, outside billing and computer services, and government, but also

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.

Box 2-D-Private Sector Computerization of Health Care Information

Medical Information Bureau

The Medical Information Bureau (MIB) was established in 1902 by a group of 15 life insurance companies. Now located in Westwood Massachusetts, the object of the industry-supported MIB is to keep underwriting costs down by uncovering dishonest or forgetful applicants for insurance. MIB's stated purpose is to discourage fraud when companies are called onto write insurance for applicants with conditions significant to longevity or insurability. MIB acts as a medical and other risk information clearinghouse for member companies. About 700 U.S. and Canadian life insurance companies at 1,054 locations belong to MIB. According to MIB, its ranks now include virtually every major company issuing individual life, health and disability insurance in the United States and Canada.[1]

While MIB was setup by and forlife insurance companies, a member of MIB can also access its file for health or disability insurance purposes if the member sells those products. information about persons applying for individual health insurance through a member of MIB can be entered into MIB.

Applications for individual insurance-health, life, ordisability-carry an explanation about MIB. If an insurance company finds something in an applicant's history that could affect longevity, the member company must file a report with MIB about the applicant's insurability y. A potential insurer may request an MIB check to see if past reports about the applicant have been filed by other companies; MIB makes about 22 million such checks each year for member insurers. MIB's reports alert a potential insurer to omissions or misrepresentation of facts by an applicant. In principle, an applicant can refuse to allow his or her information to be communicated to MIB. The price of such a refusal to an applicant is usually refusal by the insurance company to process the application.

MIB keeps its medical reports on patients for 7 years. MIB stores its records in a specially coded format, which the company will not disclose to regulators, legislators, or consumergmupson the grounds that to do so would compromise the firm's confidentiality.[2] (MIB did, however, make its code list without numerical security codes available to about SIX government organizations including the FTC on a proprietary, confidential and privileged basis).[3] MIBenters approximately 3 million coded records a year and has information on about 15 million persons in t he United States. The basic identifiers are limited to the person's name, birthdate, birth-State, occupation, and a single letter, usually signifying residence in a multi-State region such as New England. Street, mail address or telephone numbers are never included. Social Security numbers (SSN) presently are not included on MIB reports, but this may change.[4] Information about applicants is encoded into a set of 210 medical categories and 5 nonmedicai codes (e.g., hazardous sports, aviation activities, poor driving record) at the time an individual applies for medically underwitten life, health, or disability insurance from a member company. MIB does not validate the accuracy of the information. Not all information entered into MIB is negative information about an applicant, as normal results of tests are also submitted to MIB. For example, if an applicant has a previous record for high blood pressure, an entry might be made at a later date reflecting a normal blood pressure reading. Insurance claims made by individuals are not a source of records and codes for MIB.

---

1 MIB, Inc., A Consumer's Guide, Publication of the Medical Information Bureau, November 1990, p. 5. However, Blue Cross and Blue Shield do not belong to MIB.

2 Simson L. Garfinkel, "From Database to Blacklist," *The Christian Science Monitor*, Aug. 1, 1990, p. 12.

3 Neil Day, President, MIB Inc., personal communication, April 1993.

4 MIB, Inc.: A Consumer's Guide, publication of the Medical information Bureau, p. 6. However, MIB states that, after further study, use of the Social Security number has become less likely.

According to MIB, the organization attempts to maintain a reasonable balance between a person's right to privacy and an insurer's need for protection against fraud or omission. Among the safeguards it has established to protect confidentiality are its computer system that is "exceptionally user unfriendly" to the 1000 terminals in its network. MIB verifies that reports are properly requested and transmitted, and it documents all access to MIB. According to MIB, its staff of 200 is educated as to expectations of confidentiality and is limited in its access to the MIB code book, to the computer room, and the MIB database, Member companies of MIB must make an annual agreement and pledge to protect confidentiality, and are required to adhere to confidentiality requirements.

Any individual can inquire whether MIB retains a record on him or her. Individuals can inspect and seek correction of their own records. According to MIB, on average, 48,000 people request disclosure annually,[5] and after reviews conducted by the insurers who originally sent the disputed information to MIB, about 400 records are corrected.[6] MIB retains records on an individual for 7 years, if no additional reports come to MIB during that time, the record is purged.

MIB emphasizes that its reports are not used as the basis for a decision to reject an application or to increase the cost of insurance premiums. Actual underwriting decisions are based on information from the applicant and from medical professionals, hospital records, and laboratory results. In 12 States it is illegal under the National Association of Insurance Commissioners Insurance Information and Privacy Protection Model Act to make underwriting decisions solely on the content of an MIB record; the act also is adhered to by some insurers in States that have not enacted it. Another deterrent to using MIB codes to deny coverage is the requirement that insurers disclose the basis for an adverse underwriting decision under the Federal Fair Credit Reporting Act (Public Law 101 -50).

Physician Computer Network, Inc.

Physician Computer Network, Inc. (PCN) operates a national, interactive communications network linking its 2,000 office-based physician members to a variety of healthcare organizations including hospitals, clinical laboratories, Medicare/Medicaid intermediaries, Blue Cross/Blue Shield providers, managed care providers, insurance carriers, and pharmaceutical companies. For a yearly fee of approximately $3,000, PCN provides member physicians with software, peripherals, computer hardware (an IBM Personal System/2 Model 30 for the physician and a PS/2 Model 80 running Unix as the server) installation, computer training, maintenance, and telephone support for the system.

The PCN system then acts as a computer gateway link with financial management services (including patient and insurance billing and receivables), office management and administration (including word processing and scheduling), relational database manager (managing medical records, patient charts and prescriptions), practice analysis reports, interfaces with hospitals and laboratories, and electronic claims processing. In return for these services, the physician pays the relatively modest enrollment and rental fees, and agrees to watch certain promotional/educationai materiais, keep patient records on the system, and allow the aggregate clinical data to be used by PCN for some time in the future, for commercial purposes (see figure 2-D-l).

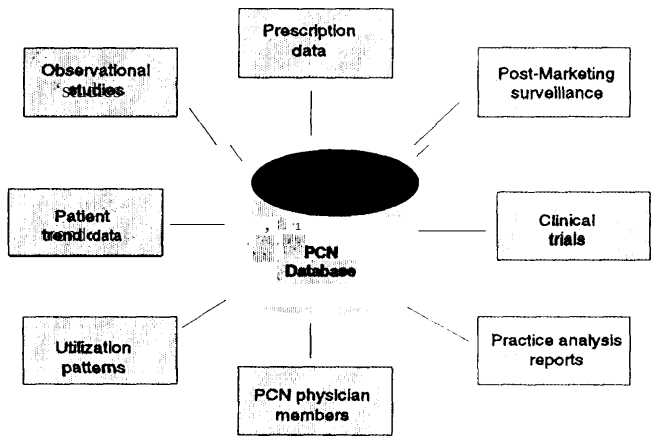
5 Michael Day, President, MIB, Inc., personal communication, April 1993.

6 According to MIB, the company is required to change records that are not correct under the Fair Credit Reporting Act. Ibid,

(continued on next page)

Box 2-D—Private Sector Computerization of Health Care Information-Continued

Figure 2-D-I—Information Services/Market Research Applications



KEY: PCN=Physicians Computer Network
SOURCE: PCN, Inc.

The PCN Electronic Communications Data-Link Service attempts to ease the burden of rising administrative costs by providing "point-to-point" electronic insurance claims processing for physicians in the New York State, Alabama and New Jersey areas. PCN plans to expand this electronic claims processing capability to Pennsylvania, Georgia, Florida and California.

The PCN Clinical Database and Market Research/Medical Information Services has been the subject of some controversy. PCN has investigated and planned for the development of a database for the purpose of providing market-related clinical data and information relevant to the office-based physician's activities and clinical trends. Under its agreement with physician members, PCN can electronically access anonymous, aggregate clinical data from the practice's databases, and can use or sell this data to market research providers, information services and other organizations. According to PCN'S 1991 Annual Report, "[u]nlike drug prescription databases derived from other sources, such as wholesaler, pharmacy and mail order prescription services, the database available to PCN consists not only of prescription information, but also includes diagnoses, treatments and procedures, as well as patient and practice demographics."

PCN sees its end users of the PCN-sourced data products as pharmaceutical manufacturers, insurance companies, health maintenance organizations and other health care institutions. By virtue of the Physician Member Agreement, entered into by the physician member and PCN, PCN has the right to market the anonymous, aggregate clinical data contained in the databases of its physician members. in anticipation of marketing this data in the future, PCN has implemented international security and has engaged in the services of a certified public accounting firm to certify that the data PCN retrieves remains anonymous. PCN also is investigating the possibility of establishing a Confidential Data Intermediary (CDI) to act as guarantor that aggregate data is, in fact, anonymous.

PCS Health Systems, Inc.

PCS Health Systems, Inc., is a managed prescription drug care company, which processes payments for companies that give their employees a PCS insurance card to present at pharmacies. In doing so, PCS looks at 120 million prescriptions a year. Ninety-five percent of pharmacies are online with PCS. These pharmacies agree to PCS participant standards, and range from large chain stores to individuality owned ones. PCS does not engage in its own underwriting; rather, PCS' customers are third-party payers with prescription drug benefit programs. PCSprocessed claims for these third-party payers. The PCSsystem involves a card system for identification and for establishment of eligibility and

level of benefits. At the time the card is presented at the pharmacy, the claim is processed and any co-payment is collected. Records of these transactions are maintained to provide for drug utilization and review, and certain information is aggregated, "sterilized" and used for marketing and academic purposes. According to PCS, the entire database is sold to PDS, a division of Walsh America, a medical information collector, without patient names *or* social securit y numbers.[7] According to Walsh, patient information is frequently compiled for pharmaceutical market research purposes. Studies to view patient compliance, drug concomitance and demographics are vital to the market research needs of many pharmaceutical companies and drug researchers.[8] In none of these studies is it important to know *or* personally identify the patient. The need is only to be able to match prescriptions to a "unit of observation" without any means of specific identity. Walsh claims that is will only accept and use patient/drug data when the information is provided in a form in which the patient cannot be identified.

In order to address the question of confidentiality in patient data, PCS issues a Data Security Manual, that includes a "PCS Employee Data Security Agreement," which is signed by PCS employees. Violation of this agreement to comply with the guidelines stated in the Data Security Manual maybe cause for disciplinary action. The Data Security Manual sets forth the purpose of the data security policies and procedures as the minimization of exposures to data and data processing resources due to errors, purposeful acts and disasters resulting in loss of assets or service to customers, It establishes a data security administration, which is responsible for, among other things, administration and control of security software systems, establishment and maintenance of the PCS corporate security policy and manual, monitoring and reporting violations of data and physical security, establishing and maintaining data security standards and procedures, password management guidelines, access rules detailing who has access to which datasets/transactions, and participation in the development of automated applications, providing data security guidance where needed. The Manual discusses the separation of functions between the Information Security Department and the user organizations, as well as within the Information Security Data Department. PCS sets forth access and security standards, including provisions for physical security, access to hardware, access to files and access to documentation. The manual also discusses policies regarding passwords, logon IDs, automatic cancellation of terminals after 15 minutes of nonuse, investigation of attempted violations to access unauthorized data, and shredding of hardcopy,

---

7 PCS had originally developed a policy, at a time when PDS was a PCS subsidiary, of transmitting the database to PDS with social security number included, with PDS encrypting the numbers before transmitting the data to any third party. A *Wall* Street *Journal* article, published Feb. 27, 1992, asserts that this policy was employed at that time. PCS comments on this situation further that when the Wall Street Journal article was published, PDS was independent of PCS but was located physically on PCS premises. However, according to PCS, the data processing functions of both organizations were performed on the same hardware as an integrated operation. While technically the responsibility for encrypting the data remained with PDS, even after it was no longer a subsidiary of PCS, the procedure was so automated and the process so fully integrated between the two organizations, that as a practical matter PDS staffs were not even aware that they *were* receiving unencrypted data When PDS and PCS became aware of this situation, the technical responsibility for data encryption was reassigned to PCS. PDS, as of October 1992 no longer occupies space at the PCS site and the data processing operations of the two firms are separate. Stephan E. Chertoff, Director, Government Relations, PCS Health Systems, personal communication, April 1993.

8 "Doctors' and Pharmacies Files are Gathered and Mined for Use by Drug Makers," *The Wall Street Journal*, Feb. 27, 1992, p. Al.

SOURCES: Jerry Brager, Chairman and Chief Executive Officer, Physician Computer Network, Inc. personal communication, January 1993, and PCN documents; Stephan Chertoff, PCS Health Systems, inc., personal communication, February 1993; and cited footnotes.

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?[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.[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.[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.[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.[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.[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.[29]

ISSUES RAISED BY COMPUTERIZATION

In view of the report by the Krever Commission, discussed inbox 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*

---

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.

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.[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 readily. This could result in a proliferation of data and information that is easily searchable.

9 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.[31]
- Computers create the potential for the easy linking of data that were not intended to be collated .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.[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.[34] The compilation of data and the ease with which the information contained in the databank can be transferre by computer make access to that information easier and more attractive to a wider group of people.[35]

---

30 OTA Workshop, July 31, 1992. Insurers' requests may be specific while the response to the request maybe 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 @fr. Commission of Inquiry Into the Confidentiality of Health Information, op. cit., footnote 31.

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

RIGHT TO PRIVACY IN HEALTH CARE INFORMATION

Privacy in health care information has traditionally 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).

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 AmericanMedical 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."[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-identtilable 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 physi-

36 AMA Principles of Medical Ethics, Principle IV.

Box 2-E–Development of the Right to Privacy in Information

Although a right to privacy is not set forth in the Bill of Rights, the Supreme Court has protected various privacy interests. The Court has found sources for a right to privacy in the First, Third, Fourth, Fifth and Ninth Amendments. The concept of privacy as a legal interest deserving an independent remedy was first enunciated in an article co-authored by Samuel Warren and Louis Brandeis in 1890,[1] which describes it as "the right to be let alone."2 Since the late 1950s, the Supreme Court has upheld a series of privacy interests under the First Amendment and due process clause, for example, "associational privacy,"3 "political privacy,"4 and the "right to anonymity in public expression."5 The Fourth Amendment protection against "unreasonable searches and seizures" also has a privacy component. In Katz v. *United States,* the Court recognized the privacy interests that protected an individual against electronic surveillance. But the Court cautioned that:

> . . . the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the constitution protect personal privacy from other forms of governmental invasion.[6]

The Fifth Amendment protection against self incrimination involves a right to privacy against unreasonable surveillance or compulsory disclosure.[7]

Until *Griswoldv. Connecticut,* 381 U.S. 479 (1985), any protection of privacy was simply viewed as essential to the protection of other more well-established rights. In *Griswold,* the Court struck down a Connecticut statute that prohibited the prescription or use of contraceptives as an infringement on marital privacy. Justice Douglas, in writing the majority opinion, viewed the case as concerning "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees," i.e., the First, Third, Fourth, Fifth and Ninth Amendments, each of which creates "zones" or "penumbras" of privacy. The majority supported the notion of an independent right of privacy inhering in the marriage relationship. Not all agreed with Justice Douglas as to its source; Justices Goldberg, Warren, and Brennan preferred to locate the right under the Ninth Amendment.

In *Eisenstadtv. Baird, 405* U.S. 438 (1972),8 the Court extended the right to privacy beyond the marriage relationship to lodge in the individual:

> If the right of the individual means anything, it is the right of the *individual,* married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.

---

1 Warren & Brandeis, *The Right to Privacy,* 4 Harvard Law Review, 193 (1890).

2 The term "the right to be let alone" was borrowed by the authors from the 19th century legal scholar and jurist Thomas Cooley. See T. Cooley, Law of Torts 29 (2d ed. 1888).

3 *NAACP* v. *Alabama* 357 U.S. 449 (1958).

4 *Watkins* v. Unite *States* 354 U.S. 178 (1957), and *Sweezy* v. *New Hampshire, 354* U.S. *234* (1957).

5 *Talley* v. *California, 362* U.S. *60* (1960).

6 *Katz* v. *United States 389* U.S. 347,350 (1967).

7 See *Escobedo* v. *Illinois,* 378 U.S. 478 (1964), *Miranda* v. *Arizona,* 384 U.S. 436 (1966); and *Schmerber v. California, 384* U.S. 757 (1966).

8 In which the Court struck down a Massachusetts law that made it a felony to prescribe or distribute contraceptives to single persons.

(continued on next page)

Box 2-E—Development of the Right to Privacy in Information-Continued

Roev. Wade, 410 U.S.113 (1973),[9] further extended the right of privacy "to en compass a woman's decision whether or not to terminate her pregnancy." The court argued that the right of privacy was "founded in the Fourteenth Amendment's concept of personal liberty and restrictions on State action." The District Court had argued that the source of the right was the Ninth amendment's reservation of the right to the people.

In the earliest case that raised the issue of the legitimate uses of computerized personal information systems, the Supreme Court avoided the central question of whether the Army's maintenance of such a system for domestic surveillance purposes "chilled" the first amendment rights of those whose names were contained in the system.[10] In two cases decided in 1976, the Court did not recognize either a constitutional right to privacy that protected erroneous information in a flyer listing active shoplifters 11 or one that protected the individual's interests with respect to bank records.[12] In *Paul v. Datis,* the court specified areas of personal privacy considered "fundamental":

> . . . matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.

Davis' claim of constitutional protection against disclosure of his arrest on a shoplifting charge was "far afield from this line of decisions" and the Court stated that it "declined to enlarge them in this manner."[13] In *United States v. Mi//er,* the Court rejected Miller's claim that he had a Fourth amendment reasonable expectation of privacy in the records kept by banks "because they are merely copies of personal records that were made available to the banks for a limited purpose," and ruled instead that "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[14]

---

9 In which the Court struck down the Texas abortion statute.

10 *Laird* v. *Tatum* 408 U.S. 1 (1972).

11 *Paul* v. *Davis* 424 U.S. 693 (1976).

12 United States v. *Miller* 425 U.S. 435 (1976).

13 Ibid., p. 713.

14 *U.S.* v. *Miller,* 425 U.S. 435, 442 (1976). In response to this decision Congress passed the Right to Financial Privacy Act of 1978 (Public Law 95-830) providing bank customers with some privacy regarding records held by banks and other financial institutions and providing procedures whereby Federal agencies can gain access to such procedures.

SOURCE: U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy,* OTA-CIT-296 (Washington D. C.: U.S. Government Printing Office, June 1986).

cian 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 confi-

dences 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.[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.

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[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.[39] The purpose of the Privacy Act is "to provide certain safeguards for an individual against an invasion of privacy.[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.

---

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 (o 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 payers 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 a 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 identifying 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).

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 records 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.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 fuded facilities.[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.[43] The regulations define apatient's record as 'any information, whether or not relating to a patient, received or acquired by a federally assisted alcohol or drug program. [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).[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. sees. 401.101-401.152, supplement and are consistent with the regulations that implement the Federal Freedom of Information Act.[46]

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

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. sees. 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).

and tend to injure that person's reputation.[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.[48]

Breach of Contract. Courts have, of late, demonstrated a willingness to apply the ethic

by secondary users of that data: parties that use medical records for nonmedical purposes. This patchwork of law addressing the question of privacy impersonal 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.[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. . . IC]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 framework. The result: a morass of erratic law, both statutory and judicial, defining the confidentiality of health information.[55]

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-l). 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 shortcomings 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

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.

Box 2-F-Recordkeeping and Information Flow In Health Care Data

Medical recordkeeping usually begins with an individual patient's personal physician, hospital, health center, or clinic. Traditionally, record keeping in the office of the physician has varied depending on medical philosophies, the nature of the medical practice, and the idiosyncrasies of the physician; some physicians use their office *records* only to jog their memories about the social and medical characteristics of the patients, while others may keep records that are very detailed in descriptions, diagnosis, and treatment. Participation in a group practice may affect the physician's habits of record keeping, since there is likely to be a greater need for clear communication between physicians in the group responsible for the patient's care. Psychiatrists, psychologists and psychotherapists in private practice vary in the amount of detail they include in the patient record, from very detailed records, including notes of physical ailments, to coded shorthand notes, *to no* written record at all.

Among the physician's considerations in determlning the manner in which he or she keeps records is the requirement of insurance companies to justify payment for services and public reporting requirements under State statutes. In addition to the need for records to comply with government requirements that the incidence of certain communicable diseases, child abuse and neglect, and accidental and industrial deaths, physicians must keep a record of their prescriptions for certain narcotics and controlled substances. The increase in filings of malpractice suites has led to the practice of 'defensive medicine,' the ordering of tests and consultations so that the record will show the doctor undertook all reasonable measures. This practice is reflected in office records, which as a result are a prime source of information about the quality of care.

The medical records kept by hospitals about admitted 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. 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 treatment decisions; alcohol and drug use; and comments on attitudes toward illness, physicians, treatments, compliance with therapy and advice, etc. Staff comments about the patient's character or demeanor are sometimes included in the record.

In addition to the central record, files maybe maintained in several departments of a hospital, including such departments as social service, billing, *and* pharmacy. Information kept in one such file may also be of relevance in another, so that the patient's hospital record becomes several different files that may overlap and are often maintained in separate places.

Hospital records are *subject* to both internal and external review. In instances such as Medicaid or Medicare, where Federal money is disbursed for health cafe, Federal regulations require the establishment of a Professional Review Organization (PRO) to determine that facilities and professional services are used properly.[1] Medical records play a central role in this process. Local and State agencies also conduct hospital reviews. The Joint Commission on Accreditation of Health Care Organizations makes considerable use of patient records when reviewing hospital facilities and procedures.

[1] The Social Security Act, Sections 1151-64.

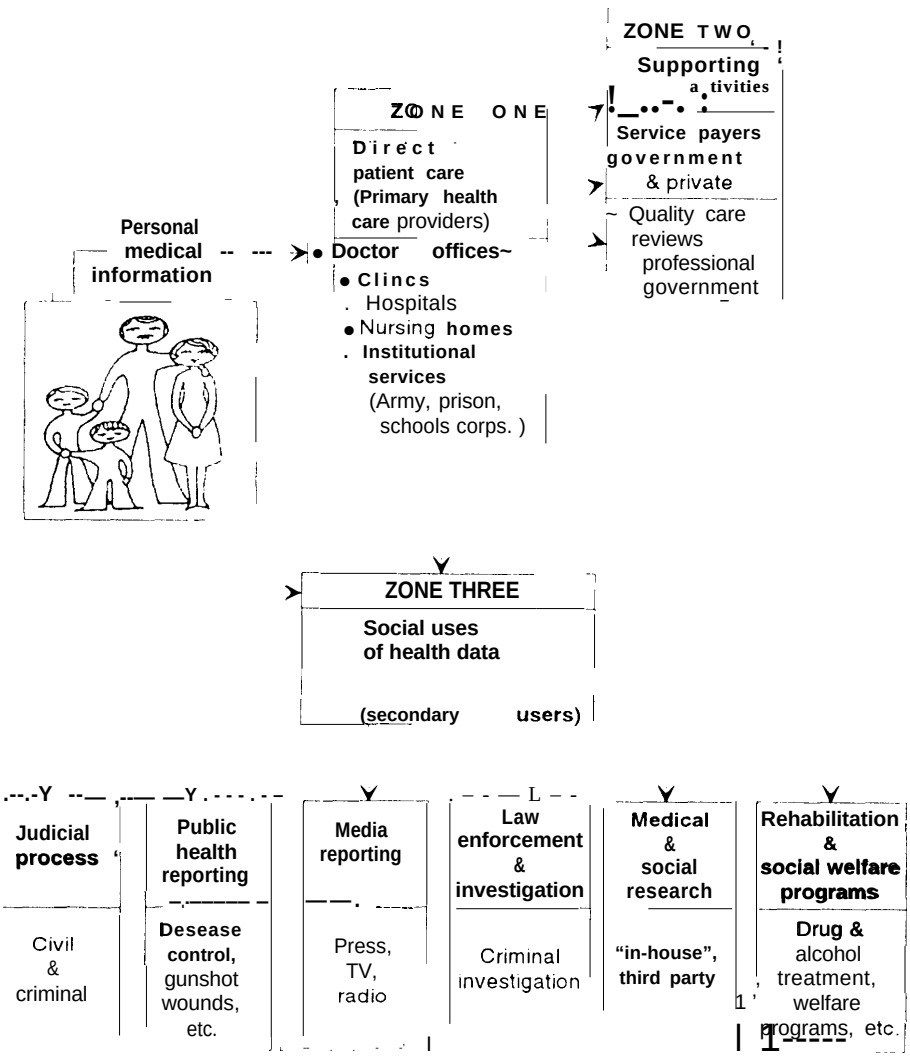
(continued on next page)

Box 2-F-Recordkeeping and Information Flow In Health Care Data-Continued

That organization sets standards for hospital accreditation, requires that standard nomenolature be used in diagnoses, and requires that records contain information sufficient to Justify a diagnosis and to warrant the choice of treatment and outcome

Thus, like private practitioners' records, hospital records are used for insuranoe, both private and governmental, protection against malpractice claims, and quality assurance. Hospitals are also subject to the same public reporting requirements as private physicians: communicable disease, law enforcement, child abuse, controlled substance prescriptions, and birth and death certificates.

Figure 2-F-l—The Flow of Personal Medical Data



SOURCE: Alan F. Westin, Computers, *Health Records, and Citizen Rights,* report prepared for the U.S. Department of Commerce, National Bureau of Standards, Monograph 157, December 1976, p. 10,

Third-Party Payers and Health Care Reviews

Medical records are used by those who pay for medical care-third party payers~both private insurance companies and government programs such as Medicare and Medicaid. Groups and government agencies that review individual medical records as part of their attempt to analyze the quality of medical care and to determine whether hospitals and other health providers are in fact delivering the health care for which they are being reimbursed also have access to medical records.

Third-party payers, whether government agencies or private companies, require positive identification of the patient and what medical services he or she received. Without this basic information, claims for benefits or reimbursement are not honored. Frequently, third party payers require more than this basic information to protect themselves against fraud by the patient or by the health care provider. Private companies may also collect medical information and other personal data in advance of granting insurance coverage underwriting to make sure that the individual is an appropriate financial and medical risk.

The three types of information generally collected by the third-party payorfrom the patient record are:

1. patient identification, including name, address, name of subscriber, relationship of patient to subscriber, patient's occupation and employer, age, sex and identifying number;
2. clinical information, including attending physician, referring physician, description of accident or illness, description of operations or medical procedure, dates of service and final diagnosis and complications; and
3. financial information, including length of stay, charge per day, and accommodations.

Hospitals and outside monitoring agencies attempt to determ ine how the hospital's facilities are being used by means of *utilization review.* The examination of whether the treatment prescribed for the patient is appropriate, and whether the actual delivery of that treatment is appropriate according to professional standards,is involved in quality care assurance. Hospitals carry out these kinds of reviews in order to plan the most efficient use of their facilities at the lowest costs. Third party payers engage in these examinations to control health care costs and to assure that good quality medical care is delivered.

Among the kinds of utilization reviews carried out is that of the Joint Commission on Accreditation of Hospitals, which reviews hospital performance to make sure that they meet certain professional standards. State and local agencies responsible for monitoring hospitals supervise sanitary facilities, compliance with building, fire and safety codes; as well as costs, procedures and length of stay.

Professional review organizations, physician staffed and directed commissions under the aegis of State Medical societies, are designed to detect fraud and misuse of facilities by health care providers and to assure that proper standards of care are secured under public funds.

Secondary Users of Personal Medical Data

The power of computers to facilitate gathering, exchanging and transmitting data could spur increased demands for use of medical information ***beyond the more traditional uses described above.*** Secondary users of personal health care data are parties that use medical records for purposes not directly involved in providing health care, paying for it or assuring its proper delivery. Rather, such information is obtained for various business or governmental purposes. Among these secondary users are life and auto insurers, employers, licensing agencies, public health agencies, the media, medical researchers, education institutions, and rehabilitation and social welfare programs. The flow of

(continued on netipage)

Box 2-F—Recordkeeping and Information Flow In Health Care Data-Continued

information to these parties in some cases affects people% lives in very direct ways, determining whether they are hired or fired, whether they can secure business iicenses and life insurances, whether they are permitted to drive cars, whether theyare piaced under policesurveillance **or labelled as security risks. Medical records are also used in civil and criminal judicial proceedings, and in quasi-judicial proceedings such as disability hearings, probation hearings, and workmen's compensation reviews.** ***Protection of privacy in computerized medical information also invovles the responsibilities of* these *secondary users in maintaining confidentially in the information.***

As discussed earlier, medical records are used to comply with public health reporting requirements. Law enforcement sees patient medical records as aresource in solving cases. Medical records are maintained as part of school records, and medical research has long been viewed as a worthwhile reason to allow access to petsonal medical information. (figure 2-F-l) ***Computers may well force in society to make clear value choices about to whom this information is made availble. Security easures such as audit trails, etc., alow the enforcement of these decisions.***[2]

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

SOURCE: Alan F. Westin, ***Computers, Health Records, and Citizen Rights,*** **National Bureau of Standards Monograph 157 (Washington, DC: U.S. Government Printing Office, 1976).**

disclosure of information but ignore the problem of subsequent disclosures .56

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

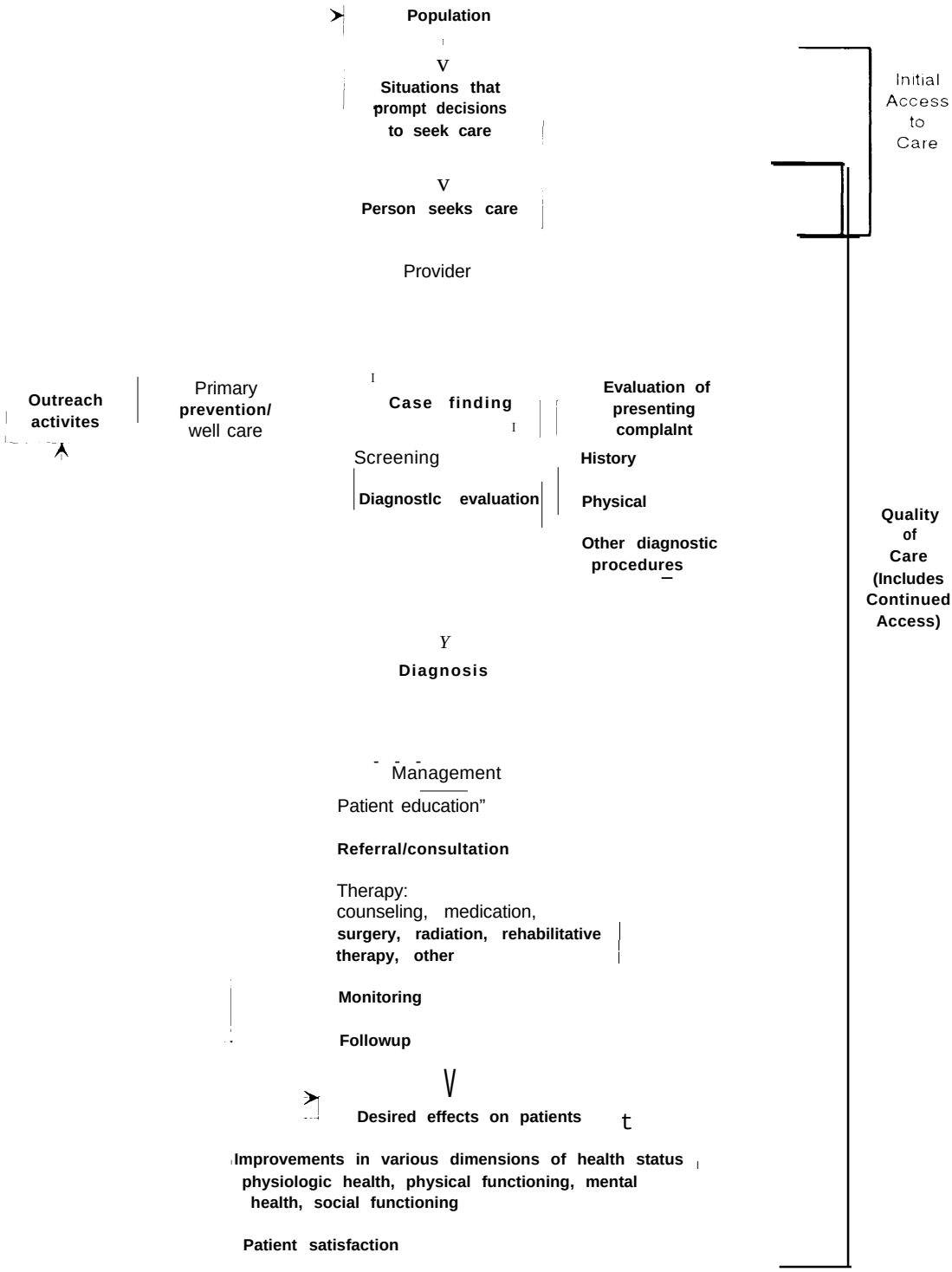
Patient awareness that records are maintained on computers, absent the assurance of a clear law protecting the confidentiality of those records, could lead to deterioration of the traditionally cofidential ''physician-patient' relationship.[57] Some contend that this breakdown could well lead to patients' 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.[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

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.

Figure 2-l—Progression of a Person Through the Spectrum of Medical Care



SOURCE: Office of Technology Assessment, 1993,

private medical settings.[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 .60

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. 2%, 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.

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.

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.

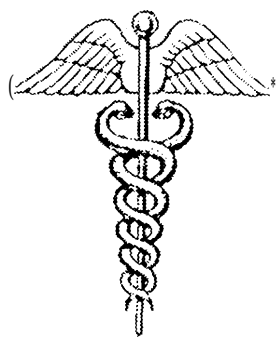
THE TECHNOLOGY OF COMPUTERIZED HEALTH CARE INFORMATION

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.

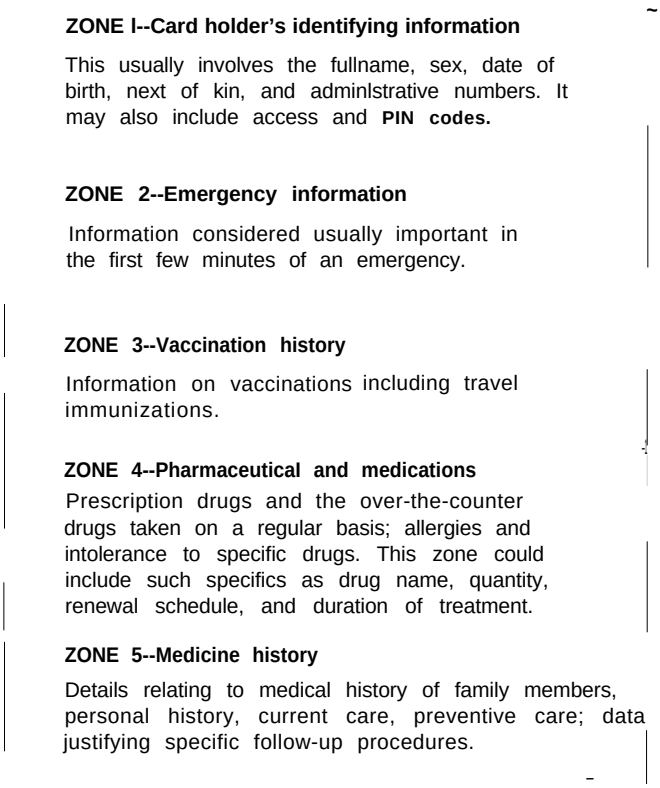
[12] Smart cards and access technologies are only one part of an overall computer security program. For a discussion of computer security measures, see app A

[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.**

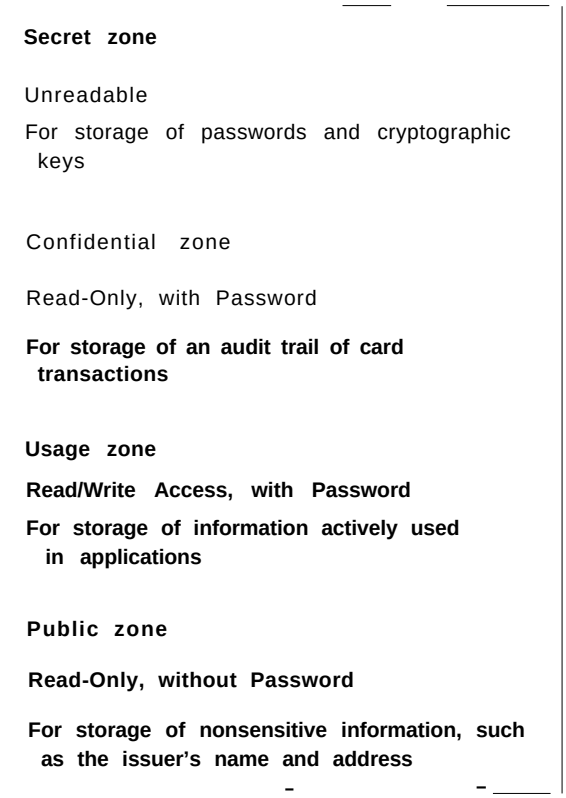
Zone 1: Identification information. All care providers would have access to this level. Only physicians, pharmacists and the issuing organization would be permitted to make entries.
Zone 2: Emergency information. All care providers would be authorized to read this zone. Only physicians would be authorized 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.

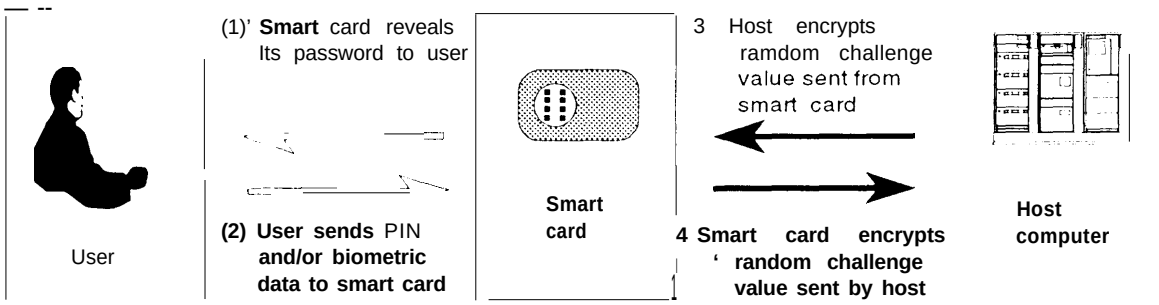
Crucial secret information can be maintained in separate protected memory locations through the use of the smart card's memory zones. It may also be possible to produce a smart card that would ensure that the entire secret zone will be destroyed if any attempt is made to access the data in that zone;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

Designing Protection for Computerized Health Care Information

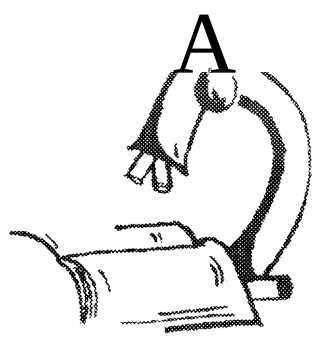
4

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.[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



[1] OTA Workshop, "Designing Privacy in Computerized Medical Information+' Dec. 7, 1992,

Box 4-A-Model Codes for Protection of Health Care Information

Proposed codes, model statutes, and legislation enacted to protect privacy in health care information are largely based on principles of fair information practices. The following briefly summarizes the purpose and applicability y of major initiatives relied on in this chapter to address features of health care information privacy legislation. The complete text of the initiatives is included in Appendix B.

Chapter 1751 of the Massachusetts State Code-Insurance Information and Privacy Protection

Massachusetts law regarding information practices and protection of privacy in insurance information is based in large part on model rules proposed by the National Association of Insurance Commissioners (NAIC). While several States have adopted the NAIC rules, Massachusetts law provides an even higher level of protection than that provided by the NAIC model. While this law was drafted specifically to address the problems of life, health, and disability insurance information, many of the definitions, principles, and provisions are equally applicable to providing privacy protection for health care information generally.

Ethical Tenets for Protection of Confidential Clinical Data

The Ethical Tenets focus directly on maintenance of the clinical data in a computerized environment.[1] while these Tenets have not been enacted into law in any jurisdiction, like the ethical codes discussed in chapter 2, they set forth guidelines that may serve as a model for legislation. In particular, the Tenets attempt to delineate what is subject to protection and what is meant by the requirement to maintain information in strict confidence. They address in some detail the issues of

[1] The Ethical Tenets were developed by a Joint Task Group on Confidentiality of Computerized Records, created in 1968. Dr. Elmer Gabrielli chaired the Task Group. When the work was completed, the Medical Society of the State of New York approved the proposal, and it remains the official guideline for the medical professionin the State of New York. Elmer Gabrieli, personal communication, April 1993.

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

informed consent, patient access to his or her medical record, and patient education about the record-keeping process. In addition, they suggest a regulatory scheme to assure proper confidentiality y and security procedures are established and maintained, using internal and external oversight groups. Unlike the more general approach of the Privacy Act, the Ethical Tenets speak directly to specific concerns encountered in the area of health care information. However, the Tenets have never had the force of law in any jurisdiction.

Uniform Health Care Information Act

The Uniform Health Care Information Act (UHCIA) has been enacted in Montana and Washington, and addresses at the State level concerns about privacy in medical information. It does not, however, focus specifically on the problems presented by computerization of this information. Many of the provisions of the UHCIA are applicable in both a computerized or noncomputerized environment. The provisions of this act are lim ited, however, to providers and hospitals in a relationship with the patient. It does not address secondary uses of health care information.

The American Health Information Management Association's Health Information Model Legislation Language

Draft model language has been proposed by AHIMA to address concerns about movement of patients and their health care information across State lines, access to and exchange of health care information from automated data banks and networks, and the emergence of multi-state health care providers and payers. It is based on the patients' need to access their own health care information and the need for clear rules about disclosure of that information. The model language also addresses proper use and disclosure of healt h care information by secondary users. It specifically sets forth its standards for information practices, incorporating principles of the patient's right to know, restrictions on collection and use only for lawful purpose, notification to patient, restriction on use for other purposes, right to access, and required safeguards. However, it provides for no oversight or enforcement mechanism for the system.

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

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.

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.[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.[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. Thereaffter, 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

[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 SIX. 552a(k)(2).

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,[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.[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 amendment.
7. The health care personnel must decide whether to amend the information within a fixed time, usually 30 days after receiving a request.
8. The individual whose request for change is denied may file a statement of disagreement, which must be included in the record and disclosed along with it thereafter.
9. The individual can seek review of a denied request.

An earlier OTA report, *Electronic Record Systems and Individual Privacy (1986)*[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).

FEATURES OF HEALTH CARE PRIVACY LEGISLATION

Congress has acted in other areas to protect the confidentiality of nongovernmental records. The

[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. 190201.

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

Right to Financial Privacy Act,[7] the Family Educational Rights and Privacy Act of 1974 (popularly known as the Buckley Amendment)[8] to protect the privacy of records maintained by schools and colleges, the Fair Credit Reporting Act[9] to protect the privacy of consumers in the reporting of credit information, and the Federal Videotape Privacy Protection Act 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 in*volved in health care, not just the clinical record used for primary treatment. " [Emphasis addedll 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. 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 (beyond the contents of the medical record) located in such places as student files, pharmacy comput-

---

[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)(l),(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.

ers, 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, broke ring, 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 freed 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.[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 from 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.[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 penalties. 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 from or imprisonment for 6 months. Anyone who obtains health care information fraudulently or unlawfully and intentionally uses, sells, or transfers the information for some monetary gain is subject to frees of not more that $50,000 and imprisonment for 2 years. The

13 **Discussion of these activities in the context of computerized medical information is discussed inch. 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.

AHIMA Model Legislation also provides for civil remedies and monetary penalties. Among the civil money penalties provided for is a from 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 stakeholders indicate that for legislation to be meaningful, penalties for improper access, possession, brokering, disclosure, or sale of information must be stringent enough to deter perpetrators.[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 frees 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.[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.[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 policyholders when applying for coverage and renewing or reinstating policies. The notice must include:

---

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

16 The code alsomakes 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).

1. whether personal information may be collected from persons other than the individual proposed for coverage;
2. the type of personal information that maybe 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 recordkeepingprocess.* 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 .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 includes patient identifiers.[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

[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 19 80, 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).

your record or get more information about it at. . , .[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* referredtoasa''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 "[identified secondary clinical records shall receive confidential treatment' '—-i. e., those records including patient identifiers such as name, address, telephone number, or Social Security number.[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

---

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 of information 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 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.

and formal authorization before information will be released.

Trubow[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'lnformation 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 spectificc 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. ' '[23] These tools include both "machine-based" and ''people-based" precautions, including concepts such as 'need to know, ' encryption,

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.

audit trails, read/write limitations, physical keys, and passwords .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 databank;
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.[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.[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

---

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 bored 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.

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.[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 functionn 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 .28

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 y remain a central concern as the health care industry contemplates full automation and implementation of a networked computer system for individual health care information.[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.*[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.[3] The level of security provided may vary from one application to another.[4] For example, security in computer systems containing classified national security information may have different specifications than a computer system designed for a nondefense 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.[5] Applications linked to external systems will usually require different security controls from those without such conections 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,

[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 Morns F. Cone% 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, 199 1), 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.

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 inforrnation.[6] A policy is implemented by taking action guided by management control principles and utilizing specific security standards, procedures, and mechanisms.[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.[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 coverall 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.[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.[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.[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.[12] In addition to these Precautions, damage can also be avoided through close personnel checks to avoid hiring employees with

---

6 See, Dennis Longley et al., op. cit., footnote 2, pp. 467468.

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.

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.

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.[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. 14

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*[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.[16] When a message is encrypted, it is encoded in a way that can be reversed only with the appropriate *key.*[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 against errors, 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 Signature & 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

---

13 See *Defending Secrets,* op. *cit. !* footnote 11, **pp. 174-180. See also,** *Datapro Reports on Information Security,* "Host File Encryption Software **Overview, " 1S54-001-101, May 1992.**

14 See generally, *Defending Secrets,* op. cit., footnote 11. See also, *Datapro Reports on Information Security,* "Host Security Software," **1S50-140-103,** November 1992, and generally, Dennis Longley et al., op. cit., foomote 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.

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.[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 decyption. 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.

Asyrnrnetric ciphers use different but related keys. One key is used to encrypt and another to decrypt a message.[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 g 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.[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.

---

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.

- 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.[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.[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.[x] After over 10 years of the public scrutiny, most experts are confident that DES is secure from virtually any adversary except a foreign government.[x] 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.[25] DES specifies a cryptographic algorithm that converts plaintextrttext 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.[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 Adelrnan. 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.[27]

9 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.[28] Authenti-

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 oft Computer Systems Technology,* June 1990.

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

24 According t. 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, NCSL Bulletin, *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,' 1S31-001-125, April 1991, and Dennis Longley et. al., op. cit., footnote 2, pp. 165-171.

28 *Defending Secrets,* op. cit., footnot 11, p. 72. See also, *Datapro Reports on information Security,* ''Host Access Control Software Overview,' 1S52-001-103, July 1992,

Box A-l–The CLIPPER Chip

On April 16,1993, the White House announced anew initiative to create encryption technology that can be used to protect proprietary information, and the privacy of personal phone conversations and electronically transmitted data. The technology is also aimed at preserving the ability of Federal, State, and local law enforcement agencies with legal authorization to conduct a wiretap to intercept phone conversations. The system involves establishment of a "key-escrow" system, in which each device containing the chip will have two unique "keys" to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" databases that will be established by the Attorney General. Access to these keys would be limited to government officials with legal authorization to conduct a wiretap.

As of this writing, public debate about the technology involved in CLIPPER Chip, as well as about the legal implications of implementing such a system continue. However, the National institute of Standards and Technology has released the following information about the CLIPPER Chip:

The CLIPPER Chip was developed by the National Security Agency. It is a hardware oriented, cryptographic device that implements asymmetric encryption/decryption algorithm and what is referred to as a "law enforcement satisfying" key escrow system. While the key escrow system design is not completely designed, the cryptographic algorithm (called SKIPJACK) is complete as of this writing (and classified SECRET).

According to the information provided by NIST, the cryptographic algorithm has the following characteristics:

1. **symmetric, 80-bit key encryption/decryption algorithm;**
2. **similar in function to Data Encryption Standard (DES);**
3. **32 rounds of processing per single encrypt/decrypt operation; and**
4. **design started by NSA in 1985; evaluation completed in 1990.**

The CLIPPER chip is just one implementation of the cryptographic algorithm. The CLIPPER Chip designed for the AT&T commercial secure voice product has the following characteristics:

1. **functions specified by NSA; logic designed by MYKOTRONX; chip fabricated by VLSI, Inc.; manufactured chip programmed (made unique) by MYKOTRONX security equipment**

cation 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

manufacturers willing to follow proper security procedures for handling and storage of the programmed chip;
2. reportedly resistant to reverse engineering, even against a sophisticated, well funded adversary;
3. 15-20 megabit per second eencryption/decryption constant throughout once cryptographic synchronization is established with distant CLIPPER Chip;
4. the chip programming equipment writes (one time) the following information into a special memory (called VROM or VIA-Link) on the chip:
   a. (unique) serial number
   b. (unique) unit key
   c. family key
   d. specialized control software
5. Upongeneration (or entry) of a session key in the chip, the chip performs the following actions:
   a. Encrypts the 80 bit session key under the unit key producing an 80 bit intermediate result;
   b. Concatenates the 80 bit result with the 25 bit serial number and a 23 bit authentication pattern (total of 128 bits);
   c. Enciphers this 128 bits with family key to produce a 128-bit cipher block chain called the Law Enforcement Field (LEF)
   d. Transmits the LEF at least once to the intended receiving CLIPPER Chip.
   e. The two communicating CLIPPER chips use this LEF to establish cryptographic synchronization.
6. Once synchronized, the CLIPPER chips use the session key to encrypt/decrypt data in both directions;
7. The chips can be programmed to not enter the secure mode if the LEF field has been tampered with (e.g., modified, superencrypted, replaced);
8. CLIPPER Chips are expected to be available from a second source in the future;
9. CLIPPER Chips are expected to be modified/ungraded in the future;
10. According to NIST CLIPPER chips presently cost $16.00 (unprogrammed) and $26.00 (programmed),

SOURCE: National Institute of Standards and Technology, Press Release, May 1993.

password or personal identification number (password authentication), or some physical characteristic of the user, e.g., a fingerprint or voice pattern (biometric authentication) .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.[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,

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.

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.[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.

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.

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.[32]

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. [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

---

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.

Box A-2–Access Control Software and Audit Trails

Access control determines who can access the system, what system resources they can access, and how they may use those resources. Adequate access control prevents users from intentionally or accidentally obtaining data without prior permission.

At the host, access control usually involves two forms of security, system *access control,* which prevents unauthorized users from logging onto the system, and *data access contro/,* which prevents authorized users from accessing and/or modifying a particular file unless the user has been given prior permission.

The following is a brief descriptive list of access control methods:

User identification. The user identification code (ID) identifies the terminal users or application programs to other applications, data, devices, or services. Access to the system or application is denied if the user name or identification code is not listed in the access control file. User IDs also enable the system to report the activities of each individual logged onto the system.

Passwords. Passwords provide for verification of the identity of users. Passwords, secret and unique codes known only tot heir owners and recognizable only to a related target system, are intended to identify the user and ensure authorized access. Permission to access a system is typically denied until the individual supplies the password assigned to the user name and access type. A system file stores passwords with the user names they reference.

Host access control software packages attempt to prevent individuals f rom guessing or otherwise improperly obtaining a password. To do this, they may:

1. specify a minimum length for passwords to prevent the creation of overiy simple passwords;
2. require users to change their passwords at regular intervals;
3. limit the number of login attempts;
4. record unsuccessful login attempts;
5. require users to accept machine-generated passwords, which can offer more security than self-generated passwords because they are randomly generated pseudo words not found in the dictionary;
6. cancel passwords that have not been used for a specified period of time;
7. perform password trapping to capture users with stolen passwords; and
8. one way encrypt the password in the system's protected password file.

Login Control Login controls specify the conditions users must meet for gaining access. In most cases, access will be perm itted only when both a username and password are provided. More complex systems grant or deny access based on the type of computer login, i.e., local, dial-up, remote, network, batch, or subprocess. The security system can restrict access based on the type of terminal or remote computer—access will only be granted when the user or program is located at a designated terminal or remote system. Also, access can be defined by time of day and day of the week. As a further precaution, the more complex systems monitor unsuccessful logins, send messages to the system operator and disable accounts when a break-in occurs.

Resource Authorization. User profiles, resource profiles, and access control lists created and maintained by t he host access control software identify the system resources to be protected, describe who can use resources, and detail the manner in which resources can be used. The protection is typically applied to applications, files, data sets, and system utilities. ft may also be applied to program processes, system commands, individual application transactions, and workstations, i.e., terminals and printers. Users and programs can have read, write, execute, delete, alter, or control access, or a

(continued on nexfpage)

Box A-2–Access Control Software and Audit Trails-Continued

combination thereof. Access authority is granted to a user or program based on whether it is an individual with unique needs or a member of a registered group.

***Authorization Checking.*Host access control packages control all interaction between the user and protected resources. The software:**

1. **intercepts access requests for resources from the operating system;**
2. **determines if the resource is protected by host access software;**
3. **references the security rights database for access profiles;**
4. **determines if the user's access request is a valid request based on the permission assigned to the user; and**
5. **passes the status of there quest tothe operating system, which then grants orden'bstheaccess request.**

***Auditing. She* breaches of security can occur *from* within an organization, and many systems can also be compromised if improper access is gained by an authorized party, accountability is key to security protection. Auditing allows a system to record significant events. Since auditing is generally tied to authentication and authorization, every authorization and attempted access is usually recorded. Examination of audit trails may also reveal suspicious patterns of access and allow detection of improper behavior by both legitimate users and impostors.**

Events that may be audited are:

1. **selected uses of files and hardware devices;**
2. **logins, logouts and break-in attempts;**
3. **activities of specific, individual users;**
4. **changes to passwords;**
5. **disk and tape value changes;**
6. **selected transaction types;**

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.[34]

[34] *Datapro Reports on Information Security* "Protecting Information by Authentication and Encryption," 1S50-140-103, June 1993.

7. issuance of system commands; and
8. changes to security profiles.

Some systems allow selection of the specific security-relevant events to be recorded. In addition, security alarms (electronic messages) can be generated to be sent immediately to the security administrator or system operator when specific events take place.

Journaling.Journaling involves recording all system activities and uses of a system resource. By analyzing this activity, the security administrator can:

1. identify access violations and the individual accountable for them,
2. determine security exposures,
3. track the activities of selected users, and
4. adjust access control measures to changing conditions.

Program and Data Integrity. Several types of controls and functions address program and data integrity:

1. Dataset naming conventions separate production data from test data. The assignment of unique types of dataset names for separate categories of data ensures that the difference between test and production data is maintained.
2. Naming conventions are also used for unique and specifically defined program names, job names, and terminal usage.
3. File placement ensures that files reside on the proper direct access storage device so that datasets do not go to a wrong device by accident
4. Program control allows only assigned programs to run in production and eliminates the problem of test programs accidentally entering the production environment.
5. Separation of production and testing ensures that no test data or programs are used in normal production.

SOURCE: Datapro Reports on Information Security, "Host Access Control," IS52-21O-1O3, July 1992.

Appendix B: Model Codes for Protection of Health Care Information

Chapter 175I of the Massachusetts State Code-Insurance Information and Privacy Protection 102-118

Ethical Tenets for Protection of Confidential Clinical Data.....l 19-126

Uniform Health Care Information Act (As codified in Chapter 16, Part 5 of the Montana Code) 127-138

The American Health Information Management Association's HeaIth Information Model Legislation Language.....,,,. 139-152

CHAPTER 1751. INSURANCE INFORMATION AND PRIVACY PROTECTION

Section
1. Application of chapter.
2. Definitions.
3. Pretext interviews; use.
4. Notice of information practices; time; contents; abbreviated notice.
5. Questions to marketing or research information; disclosure.
6. Disclosure authorization form; **contents**
7. Investigative consumer report; personal interview; prohibited information.
8. Recorded personal information; medical record information; disclosure; fees.
9. Correction, amendment or deletion of personal information.
10. Adverse underwriting decision; notice; reasons; disclosure of medical or mental health record information; summary of rights.
11. Prior adverse underwriting decisions; request for information by insurance organizations.
12. Adverse underwriting decision; basis.
13. Personal or privileged information from insurance transactions; disclosure.
14. Investigations.
15. Violations; notice; hearings; Service of process.
16. Agent for service of process.
17. Findings; orders to cease and desist; reports.
18. Penalties; violations of cease and desist orders.
19. Judicial review; filing deadline; jurisdiction; orders.
20. Equitable relief; damages; costs and attorney's fees; limitation of actions.
21. Disclosure of information; immunity.
22. Information obtained by false pretenses; penalties.

Chapter 1751 of the General Laws was added by St.1991, c. 516, 1.

1. Application of chapter

(a) The obligations imposed by this chapter shall apply to an insurance institution, insurance representative or insurance-support organization which in the case of life, health and disability insurance:

(1) collects, receives or maintains information in connection with an insurance transaction which pertains to a natural person who is a resident of the commonwealth; or

(2) engages in an insurance transaction with an applicant, individual or policyholder who is a resident of the commonwealth.

(b) In the case of life, health or disability insurance, the rights granted by this chapter shall extend to the following residents of the commonwealth:

(1) natural persons who are the subject of information collected, received or maintained in connection with insurance transactions; and

(2) applicants, individuals or policyholders who engage in or seek to engage in insurance transactions.

(c) For purposes of this section, a person shall be considered a resident of the commonwealth if such person's last known mailing address, as shown in the records of the insurance institution, insurance representative or insurance-support organization, is located in the commonwealth.

Added by St.1991, c. 516, 1.

Historical and Statutory Notes

1991 Legislation

St.l991, c. 516, $ 1, adding this chapter, consisting of this section and $$ 2 to 22, was approved Jan, 7, 1992, and by $ 3 made effective July 1, 1992.

Section 4 of St.1991, c. 516, provides:

"The provisions and scope of this act shall not extend to property casualty insurers or property casualty insurance representatives. "

$ 2. Definitions

As used in this chapter the following words shall, unless the context otherwise requires have the following meanings:

"Adverse underwriting decision", (1) any of the following actions with respect to insurance transactions involving insurance coverage which is individually underwritten:

(i) a declination of insurance coverage;

(ii) a termination of insurance coverage;

(iii) failure of an insurance representative to apply for insurance coverage with a specific insurance institution which the insurance representative represents and which is requested by an applicant; or

(iv) in the case of a life, health or disability insurance coverage, an offer to insure at higher than standard rates.

(2) Notwithstanding the provisions of clause (l), the following actions shall not be considered adverse underwriting decisions but the insurance institution *or* insurance representative responsible for their occurrence shall nevertheless provide the applicant or policyholder- with the specific reason or reasons for their occurrence:

(i) the termination of an indidiual policy form on a class or statewide basis;

(ii) a declination of insurance coverage solely because such coverage is not available on a class or statewide basis; or

(iii) the rescission of a policy.

"Affiliate" or "affiliated", a person who directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person.

"Applicant", any person who seeks to contract for insurance coverage other than a person seeking group insurance that is not individually underwritten.

"Commissioner", the commissioner of insurance or his designee.

"Consumer report", a written, oral or other communication of information bearing on a natural person's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used in connection with an insurance transaction.

"Consumer reporting agency" any person who:

(1) regularly engages, in whole *or* in part, in the practice of assembling or preparing consumer reports for a monetary fee;

(2) obtains information primarily from sources other than insurance institutions; and

(3) furnishes consumer reports to other persons.

''Control, including the terms ''controlled by' or "under common control with", the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract other than a commercial contract for goods or nonmanagement services, or otherwise unless the power is the result of an official position with or corporate office held held by the person

''Declination of insurance coverage'', a denial, in whole or in part, by an insurance institution or insurance representative of requested insurance coverage.

''Individual'', any natural person who:

(1) in the case of life, health or disability insurance, is a past present or proposed principal insured or certificate holder;

(2) is apast present or proposed policy owner;

(3) is pastor present applicantion

(4) is a past or present claimant or

(5) derived, derives or is proposed to derive insurance coverage under an insurance policy or certificate subject to this chapter.

"Institutional source", any person or governmental entity that provides information about an individual to an insurance representative, insurance institution or insurance-support organization, other than:

(1) an insurance representative;

(2) the individual who is the subjectof the information; or

(3) a natural person acting in a personal capacity rather than in a business or professional capacity.

"Insurance institution", any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's insurer, fraternal benefit society or other person engaged in the business of insurance, including health maintenance organizations, medical service plans and hospital service plans, preferred provider arrangements and Savings Bank Life Insurance as defined in chapters one hundred and seventy-five, one hundred and seventy-six, one hundred and seventy-six A, one hundred and seventy-six B, one hundred and seventy-six C, one hundred and seventy-six G,one hundred and seventy-six I, one hundred and seventy-eight and one hundred and seventy-eight A, "Insurance institution" shall not include insurance representatives or insurance-support organizations.

"Insurance-support organization":

(1) any person who regularly engages, in whole or in part, in the practice of assembling or collecting information about natural persons for the primary purpose of providing the information to an insurance institution or insurance representative for insurance transactions, including:

(i) the furnishing of consumer reports or investigative consumer reports to an insurance institution or insurance representative for use in connection with an insurance transaction; or

(ii) the collection of personal information from insurance institutions, insurance representatives or other insurance-support organizations for the purpose of detecting or preventing fraud or material misrepresentation in connection with insurance underwriting or insurance claim activity.

(2) Notwithstanding the provisions of subparagraph (l), the following persons shall not be considered "insurance-support organizations" for purposes of this chapter: insurance representatives, government institutions, insurance institutions, medical care institutions and medical professionals.

"Insurance representative", an agent, broker, advisor, adjuster or other person engaged in activities described in sections one hundred and sixty-two to one hundred and seventy-seven D, inclusive, of chapter one hundred and seventy-five.

"Insurance transaction", any transaction involving life, health or disability insurance which entails:

(1) the determination of an individual's eligibility for an insurance coverage, benefit or payment; or

(2) the servicing of an insurance application, policy, contract or certificate.

"Investigative consumer report", a consumer report or portion thereof in which information about a natural person's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with the person's neighbors, friends, associates, acquaintances or others who may have knowledge concerning such items of information, provided; however, that it shall be unlawful for any such report to

contain any information designed to determine the sexual orientation of an applicant, proposed insured, policyholder, beneficiary or any other person, or for such persons, information relating to counseling for Acquired Immune Deficiency Syndrome (AIDS) or AIDS-related Complex (ARC) as defined by the Centers for Disease Control of the United States Public Health Service. For purposes of this subsection, "counseling" shall not mean diagnosis of or treatment for AIDS or ARC.

"Medical-care institution", any facility or institution that is licensed to provide health care services to natural persons, including but not limited health-maintenance organizations, home-health agencies, hospitals, medical clinics, public health agencies, rehabilitation agencies and skilled nursing facilities.

"Medical professional", any person licensed or certified to provide health care services to natural persons, including, but not limited to, a chiropractor, clinical dietician, clinical psychologist, dentist, nurse, occupational therapist, optometrist, pharmacist, physical therapist, physician, podiatrist, psychiatric social worker or speech therapist.

"Medical-record information", personal information which:

(1) relates to an individual's physical or mental condition, medical history or medical treatment; and

(2) is obtained from a medical professional or medical-care institution, from the individual, or from such individual's spouse, parent or legal guardian;

Medical-record information shall not include information relating to counseling for Acquired Immune Deficiency Syndrome (AIDS) or AIDS-related Complex (ARC) as defined by the Centers for Disease Control of the United States Public Health Service. For purposes of this definition, "counseling" shall not mean diagnosis of or treatment for AIDS or ARC.

"Person", any natural person, corporation, association, partnership or other legal entity.

"Personal information", any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics. "Personal information" shall include an individual's name and address and "medical-record information" but shall not include "privileged information".

"Policyholder", any person who:

(1) in the case of individual life, health or disability insurance, is a present policyholder; or

(2) in the case of group life, health or disability insurance which is individually underwritten, is a present group certificate holder.

"Pretext interview", an interview by a person who attempts to obtain information about a natural person and who commit-s one *or* more of the following acts:

(1) pretends to be someone he is not;

(2) pretends to represent a person he is not in fact representing;

(3) misrepresents the true purpose of the interview; or

(4) refuses to identify himself upon request.

"Privileged information", any individully identifiable information that:

(1) relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual; and

(2) is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an indvidual; provided, however, that information otherwise meeting the requirements of this definition shall nevertheless be considered "personal information" under this chapter if it is disclosed in violation of section thirteen.

"Termination of insurance coverage" or "termination of an insurance policy", either a cancellation or nonrenewal of an insurance policy, in whole or in part, for any reason other than the failure to pay a premium as required by the policy.

"Unauthorized insurer", an insurer not lawfully admitted to issue policies of insurance or an annuity or pure endowment contract, except as provided in section one hundred and sixty of chapter one hundred and seventy-five.

Added by St.1991, c. 516, 1.

3. Pretext interviews; use

No insurance institution, insurance representative, or insurance-support organization shall use or authorize the use of pretext interviews to obtain information in connection with an insurance transaction; provided, however, that a pretext interview may be undertaken to obtain information from a person or institution that does not have a generally or statutorily recognized privileged relationship with the person about whom the information relates for the purpose of investigating a claim where, based upon specific information available for review by the commissioner, there is a reasonable basis for suspecting criminal activity, fraud or material misrepresentation in connection with the claim.

Added by St.1991, c. 516, ~ 1.

$ 4. Notice of information practices; time; contents; abbreviated notice

(a) An insurance institution or insurance representative shall provide a notice of information practices to all applicants or policyholders in connection with insurance transactions as follows:

(1) in the case of an application for insurance, a notice shall be provided no later than at the time the application for insurance is made;

(2) in the case of a policy renewal, a notice shall be provided no later than the policy renewal date, except that no notice shall be required in connection with a policy renewal if:

(i) personal information is collected only from the policyholder or from public records; or

(ii) a notice meeting the requirements of this section has been given within the previous twenty-four months;

(3) in the case of a policy reinstatement or change in insurance benefits, a notice shall be provided no later than the time a request for a policy reinstatement or change in insurance benefits is received by the insurance institution, except that no notice shall be required if personal information is collected only from the policyholder or from public records.

(b) A notice required by subsection (a) shall be in writing and shall state:

(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 type of source and investigative technique that may be used to collect such information;

(3) the type of disclosure permitted by this chapter and the circumstances under which such disclosure may be made without prior authorization; provided, however, that only such circumstances need be described which occur with such frequency as to indicate a general business practice;

(4) a description of the rights established under sections eight, nine and ten and the manner in which such rights may be exercised; and

(5) that information obtained from a report prepared by an insurance-support organization may be retained by the insurance-support organization and disclosed to other persons.

(c) In lieu of the notice prescribed in subsection (b), the insurance institution or insurance representative may provide an abbreviated notice informing the applicant or policyholder that:

(1) personal information may be collected from a person other than the individual proposed for coverage;

(2) such information as well as other personal or privileged information subsequently collected by the insurance institution or insurance representative may in certain circumstances be disclosed to a third party without authorization;

(3) a right of access and correction exists with respect to all personal information collected; and

(4) the notice prescribed in subsection (b) shall be furnished to the applicant or policyholder upon request.

(d) The obligations imposed by this section upon an insurance institution or insurance representative may be satisfied by another insurance institution or insurance representative authorized to act on its behalf.

(e) Information collection and disclosure authorized pursuant to this chapter is limited to the practices described in the notice issued or available pursuant to this section.

Added by St.1991, c. 516, $ 1.

$ 5. Questions to obtain marketing or research information; disclosure

An insurance institution or insurance representative shall clearly specify questions designed to obtain information solely for marketing or research purposes from an individual in connection with an insurance transaction.

Added by St.1991, c. 516,$ 1.

$ 6. Disclosure authorization form; **contents**

Notwithstanding any general or special law to the contrary, no insurance institution, insurance representative or insurance-support organization may utilize as its disclosure authorization form in connection with insurance transactions a form or statement which authorizes the disclosure of personal or privileged information about an individual to the insurance institution, insurance representative *or* insurance-support organization unless the form or statement:

(1) is written in plain language;

(2) is dated;

(3) specifies the types of persons authorized to disclose information about the individual;

(4) specifies the nature of the information authorized to be disclosed;

(5) names the insurance institution or insurance representative and identifies by generic reference the representative of the insurance institution to whom the individual is authorizing information to be disclosed;

(6) specifies the purposes for which the information is collected;

(7) specifies the length of time such authorization shall remain valid, which shall be no longer than:

(A) in the case of authorizations signed for the purpose of collecting information in connection with an application for an insurance policy a policy reinstatement or a request for change in policy benefits, thirty months from the date the authorization is signed; or

(B) in the case of authorizations signed for the purpose of (’collecting information in connection with a claim for benefits under an insurance policy:

(i) the term of coverage of the policy’ if the claim is for a health insurance benefit; or

(ii) the duration of the claim if the claim is not for a health insuranc(> benefit; and

(8) advises the individual or a person authorized to act on behalf of such individual that such individual or the individual's authorized representative is entitled to receive a copy of the authorization form.

Added by St.1991, c. 516, $ 1.

7. Investigative consumer report; personal interview; prohibited information

(a) No insurance institution, insurance representative or insurance-support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement or a change in insurance benefits unless the insurance institution or insurance representative informs the individual:

(1) that each individual may request to be intro-viewed in connection with the preparation of the investigative consumer report; and

(2) that upon a request pursuant to section eight, such individual is entitled to receive a copy of the investigative consumer report.

(b) If an investigative consumer report is to be prepared by an insurance institution or insurance representative, such insurance institution or insurance representative shall institute reasonable procedures to conduct a personal interview requested by an individual.

(c) If an investigative consumer report is to be prepared by an insurance-support organization, the insurance institution or insurance representative desiring such report shall inform the insurance-support organization whether a personal interview has been requested by the individual. The insurance-support organization shall institute reasonable procedures to conduct such **reviews,** if requested.

(d) No investigative consumer report shall contain any information designed to determine the sexual orientation of an applicant, proposed insured, policyholder, beneficiary or any other person, or for such persons, information relating to counseling for Acquired Immune Deficiency Syndrome (AIDS) or AIDS-related Complex (ARC) as defined by the Centers for Disease Control of the United States Public Health Service. For purposes of this subsection, "counseling" shall not mean diagnosis of or treatment for AIDS or ARC,

Added by St.1991, c. 516, $ 1.

8. Recorded personal information; medical record information; disclosure; fees

(a) An insurance institution, insurance representative or insurance-support organization shall make any personal information collected or maintained in connection with an insurance transaction in its possession or control available to the individual to whom it refers, or to the authorized representative of such individual, as provided in this section.

(b) If any individual, after identification, submits a written request to an insurance institution, insurance representative or insurance-support organization for access to recorded personal information about such individual which is reasonably described by such individual and reasonably locatable and retrievable by the insurance institution, insurance representative or insurance-support organization, the insurance institution, insurance representative or insurance-support organization shall within thirty business days from the date such request is received:

(1) either provide such individual with a copy of such recorded personal information or inform such individual of the nature and substance of such recorded personal information in writing;

(2) permit such individual to see and copy, in person, such recorded personal information or to obtain a copy of such recorded personal information by mail, whichever the individual prefers, unless such recorded personal information is in coded form, in which case an accurate translation in plain language shall be provided in writing;

(3) disclose to such individual the identity, if recorded, of any person to whom the insurance institution, insurance representative or insurance-support organization has disclosed such personal information within two years prior to such request, and if such identity is not recorded, the names of insurance institutions, insurance representatives, insurance-support organizations or other persons to whom such information is normally disclosed; and

(4) provide such individual with a summary of the procedures by which such individual may request correction, amendment or deletion of recorded personal information.

(c) Any personal information provided pursuant to subsection (b) shall contain the name or identify the source, except that a source that is a natural person acting in a personal capacity need not be revealed if such confidentiality was specifically promised.

(d) Medical record information supplied by a medical care institution or medical professional and requested under subsection (b), together with the identity of the medical professional or medical care institution which provided such information, shall be supplied either directly to the individual or to a medical professional designated by such individual and licensed to provide medical care with respect to the condition to which the information relates, whichever such individual prefers. Mental health record information shall be supplied directly to such individual, pursuant to this section, only with the approval of the qualified professional person with treatment responsibility for the condition to which the information relates or another equally qualified mental health professional. Upon release of any medical or mental health record information to a medical professional designated by such individual, the insurance institution, insurance representative or insurance-support organization shall notify such individual, at the time of the disclosure, that it has provided the information to the medical professional.

(e) Except for personal information provided under section ten, an insurance institution, insurance representative or insurance-support organization may charge a reasonable fee to cover the costs incurred in providing a copy of recorded personal information to an individual but no other fee may be charged.

(f) The obligations imposed by this section upon an insurance institution or insurance representative may be satisfied by another insurance institution or insurance representative authorized to act on its behalf. With respect to the copying and disclosure of recorded personal information pursuant to a request under subsection (b), an insurance institution, insurance representative or insurance-support organization may make arrangements with an insurance-support organization or a consumer reporting agency to copy and disclose recorded personal information on its behalf so long as the insurance-support organization or consumer reporting agency has established and maintains procedures for maintenance of records to assure confidentiality.

(g) The rights granted to an individual in this section shall extend to a natural person to the extent information about such person is collected and maintained by an insurance institution, insurance representative or insurance-support organization in connection with an insurance transaction. The rights granted to a natural person by this subsection shall not extend to information about such person that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving such person.

(h) For the purpose of this section, the term "insurance support organization" shall not include "consumer reporting agency".

Added by St.1991, c. 516, $ 1

Historical and Statutory Notes

1991Legislation

Section 2 of St.1991, c. 516, as amended by St. 1992, c. 286, $ 2'76, provides:

"Chapter 516 of the acts of 1991 is hereby amended by striking out section 2 and inserting in place thereof the following section:—

"Section 2. The provisions of sections eight, nine and thirteen of chapter one hundred and seventy-five I of the General Laws, inserted by section one of this act, shall apply to rights granted therein regardless of the date of collection *or* receipt of the information which is the subject of such sections. "

St.1992, c. 2$6, I$ 276, **an** emergency act was approved Dec. 23, 1992.

$ 9. Correction, amendment or deletion of personal information

(a) An individual to whom personal information refers has a right **to** have any factual error corrected and any misrepresentation or misleading entry amended or deleted as provided in this section.

(b) Within thirty business days from the date of receipt of a written request from an individual to correct, amend or delete any recorded personal information about such individual within its possession, an insurance institution, insurance representative or insurance-support organization shall either:

(1) correct, amend or delete the portion of the recorded personal information in dispute; or

(2) reinvestigate the disputed information and upon completion of such reinvestigation the insurance institution, insurance representative or insurance-support organization shall correct, amend or delete the portion of the recorded personal information in dispute or notify the individual of:

(i) its refusal to make such correction, amendment or deletion;

(ii) the reason for such refusal;

(iii) the individual's right to file a statement as provided in subsection (d); and

(iv) the individual's right to request review by the commissioner of insurance as provided by section fourteen.

(c) If the insurance institution, insurance representative or insurance-support organization corrects, amends or deletes recorded personal information in accordance with paragraph (1) of subsection (b), the insurance institution, insurance representative or insurance-support organization shall so notify the individual in writing and furnish the correction, amendment or fact of deletion to:

(1) any person who, according to the records of the insurance institution, insurance representative or insurance-support organization, has, within the preceding two years received such recorded personal information from the insurance institution, insurance representative or insurance-support organization, and any person specifically designated by the individual who may have, within the preceding two years, received such recorded personal information; provided, however, that this subsection shall apply only to personal information which is medical record information or which relates to the individual's character, general reputation, personal characteristics or mode of living;

(2) any insurance-support organization whose primary source of personal information is insurance institutions if the insurance-support organization has systematically received such recorded personal information from the insurance institution within the preceding seven years; provided, however, that the correction, amendment or fact of deletion need not be furnished if the insurance-support organization no longer maintains recorded personal information about the individual; and

(3) any insurance-support organization that furnished the personal information that has been corrected, amended or deleted.

(d) Whenever an individual disagrees with an insurance institution's, insurance representative's or insurance-support organization's refusal to correct, amend or delete recorded persona! information, such individual shall be permitted to file with the insurance institution, insurance representative or insurance-support organization:

(1) a concise statement setting forth what such individual thinks is the correct, relevant or fair information; and

(2) a concise statement of the reasons why such individual disagrees with the insurance institution's, insurance representative's or insurance-support organization's refusal to correct, amend or delete recorded personal information.

(e) In the event an individual files a statment as described in subsection (d), the insurance institution, insurance representative or insurance-support organization shall:

(1) file the statement with the disputed personal information and provide a means by which anyone reviewing the disputed personal information will be made aware of the individual's statement and have access to it;

(2) in any subsequent disclosure by the insurance institution, insurance representative or insurance-support organization of the recorded personal information that is the subject of disagreement, clearly identify the matter in dispute and provide the individual's statement along with the recorded personal information being disclosed; and

(3) furnish the statement to the persons and in the manner specified in subsection (c).

(f) The rights granted to an individual in this section shall extend to a natural person to the extent information about such person is collected and maintained by an insurance institution, insurance representative or insurance-support organization in connection with an insurance transaction. The right-s granted to a natural person by this subsection shall not extend to information about such person that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving such person.

(g) For purposes of this section, the term "insurance-support organization" shall not include "consumer reporting agency".

Added by St.1991, c 516, 1

Historical and **Statutory Notes**

1991 Legislation

Section 2, of **St.1991, c. 516,** as amended by St.1992, c. 286, $ 276, provides:

"Chapter 516 of the acts of 1991 is hereby amended by striking out section 2 and inserting in place thereof the following section:—

"Section 2. The provisions of sections eight, nine and thirteen of chapter one hundred and seventy-five I of the General Laws, inserted by section one of this act, shall apply to rights granted therein regardless of the date of collection or receipt of the information which is the subject of such sections. "

St.1992, c. 286, $ 276, an emergency act, was approved Dec. 23, 1992.

$ 10. **Adverse underwriting decision;** notice; reasons; disclosure of medical or mental health record information; summary of rights

(a) In the event of an adverse underwriting decision, the insurance institution or insurance representative responsible for the decision shall:

(1) either provide the applicant, policyholder or individual proposed for coverage with the specific reason for the adverse underwriting decision in writing or advise such person that upon written request such person may receive the specific reason in writing; and

(2) provide the applicant, policyholder or individual proposed for coverage with a summary of the rights established under subsection (b) and sections eight and nine.

(b) Upon receipt of a written request within ninety business days from the date of the mailing of notice or other communication of an adverse underwriting decision to an applicant, policy. holder or individual proposed for coverage, the insurance institution or insurance representative shall furnish to such person within twenty-one business days from the date of receipt of such written request:

(1) the specific reason for the adverse underwriting decision, in writing, if such information was not initially furnished in writing pursuant to paragraph (1) of subsection (a); and

(2) the specific items of personal and privileged information that support such reason; provided, however, that:

(i) the insurance institution or insurance representative shall not be required to furnish specific items of privileged information if it has a reasonable suspicion, based upon specific information available for review by the commissioner, that the applicant, policy-

holder or individual proposed for coverage has engaged in criminal activity, fraud, or material misrepresentation; and

(ii) specific items of medical record information supplied by a medical care institutionor medical professional shall be disclosed either directly to the individual about whom the information relates or to a medical professional designated by such individual and licensed to provide medical care with respect to the condition to which the information relates, whichever such individual prefers. Mental health record information shall be supplied directly to such individual, pursuant to this subsection, only with the approval of the qualified professional person with treatment responsibility for the condition to which the information relates or of another equally qualified mental health professional. Upon release of any medical or mental health record information to a medical professional designated by such individual, the insurance institution, insurance representative or insurance-support organization shall notify such individual, at the time of the disclosure, that it has provided the information to the medical professional; and

(3) the name and address of the source that supplied the specific items of information pursuant to paragraph (2) of subsection (b); except that a source that is a natural person acting in a personal capacity need not be revealed if confidentiality was specifically promised; provided, however, that the identity of any medical professional or medical-care institution shall be disclosed either directly to the individual or to the designated medical professional other than the one who initially supplied the information, whichever such individual prefers.

(c) The obligations imposed by this section upon an insurance institution or insurance representative may be satisfied by another insurance institution or insurance representative authorized to act on its behalf.

(d) When an adverse underwriting decision results solely from an oral request or inquiry, the explanation of reasons and summary of rights required by subsection (a) may be given orally.

Added by St.1991, c. 516, $ 1.

$ 11. Prior adverse underwriting decisions; requests for information by insurance organizations

No insurance institution, insurance representative or insurance-support organization may seek information in connection with an insurance transaction concerning any previous adverse underwriting decision experienced by an individual unless such inquiry also requests the reasons for any previous adverse underwriting decision.

Added by St.1991, c. 516, $ 1.

$ 12. Adverse underwriting decision; basis

No insurance institution or insurance representative may base an adverse underwriting decision in whole or in part:

(1) on the fact of a previous adverse underwriting decision or on the fact that an individual previously obtained insurance coverage through a residual market mechanism; provided, however, that an insurance institution or insurance representative may base an adverse underwriting decision on further information obtained from an insurance institution or insurance representative responsible for a previous adverse underwriting decision;

(2) on personal information received from an insurance-support organization whose primary source of information is insurance institutions; provided, howe~'er, that an insurance institution or insurance representative may- base an adverse underwriting decision on further personal information obtained as the result of information received from such insurance-support organization; or

(3) on the basis of sexual orientation; provided, however, that neither the national origin, marital status, lifestyle or living arrangements, occupation, gender, medical history, beneficiary designation, nor zip code or other territorial classification of the

applicant may be used to establish, or aid in establishing, the applicant's sexual orientation.

Added by St.1991, c. 516, $ 1.

13. Personal or privileged information from insurance transactions; disclosure

An insurance institution, insurance representative or insurance-support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is:

(1) with the written authorization of the individual, provided that:

(i) if such authorization is submitted ***by another*** insurance institution, insurance representative or insurance-support organization, the authorization meets the requirement of section six; or

(ii) if such authorization is submitted by a person other than an insurance institution, insurance representative or insurance-support organization, the authorization is:

(A) dated;

(B) signed by the individual; and

(C) obtained one year or less prior to the date a disclosure is sought pursuant to this subsection; or

(2) to a person other than an insurance institution, insurance representative or insurance-support organization; provided, however, that such disclosure is reasonably necessary:

(i) to enable such person to perform a specific business, professional or insurance function for the disclosing insurance institution, insurance representative or insurance-support organization and such person agrees not to disclose the information further without such individual's written authorization unless the further disclosure:

(A) would otherwise be permitted by this section if made by an insurance institution, insurance representative or insurance-support organization; or

(B) is reasonably necessary for such person to perform its specific business, professional or insurance function for the disclosing insurance institution, insurance representative or insurance-support organization; or

(ii) to enable such person to provide information to the disclosing insurance institution, insurance representative or insurance-support organization for the purpose of:

(A) determining an individual's eligibility for an insurance benefit or payment; or

(B) detecting or preventing criminal activity, fraud or material misrepresentation in connection with an insurance transaction; or

(3) to an insurance institution, insurance representative, or insurance-support organization; provided, however, that the information disclosed is limited to that which is reasonably necessary:

(i) to detect or prevent criminal activity, fraud or material misrepresentation in connection with insurance transactions; or

(ii) for the receiving or disclosing insurance institution, insurance representative or insurance-support organization to perform its function in connection with an insurance transaction involving an individual; provided, however, that the recipient of the information is prohibited from redisclosing the information without explicit written authorization according to the requirements of paragraph (1) or that the individual is notified, either concurrently with the application or otherwise prior to disclosure of the information, that the disclosure of the information may be made and can find if the disclosure has been made; or

(4) to a medical-care institution or medical professional for the purpose of:

(i) verifying insurance coverage or benefits; or

(ii) informing an individual of a medical problem of which the individual may not be aware; or

(iii) conducting an operations or services audit to verify the individuals treated by the medical professional or at the medical-care institution, provided only. such information is disclosed as is reasonably necessary to accomplish the foregoing purposes; or

(5) to an insurance regulatory authority; or

(6) to a law enforcement or other governmental authority:

(i) to protect the interests of the insurance institution, insurance representative or insurance-support organization in preventing or prosecuting the perpetration of fraud upon it; or

(ii) if the insurance institution, insurance representative or insurance-support organization reasonably believes that illegal activities have been conducted by the individual; or

(7) otherwise permitted or required by law; or

(8) in response to a facially valid administrative or judicial order, including a search warrant or subpoena; or

(9) made for the purpose of conducting actuarial or research studies, provided that:

(i) no individual may be identified in any actuarial or research report;

(ii) information allowing the individual to be identified is removed to the extent practicable and where such removal is not practicable, is returned or destroyed as soon as it is no longer needed; and

(iii) the actuarial or research organization agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, insurance representative or insurance-support organization and the disclosure is made in connection with such actuarial or research studies; or

(10) to a party or representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the insurance of the insurance institution, insurance representative or insurance-support organization, provided that:

(i) prior to the consummation of the sale, transfer, merger or consolidation only such information is disclosed as is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger or consolidation; and

(ii) the recipient agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, insurance representative or insurance-support organization and the disclosure is made in connection with such sale, transfer, merger or consolidation; or

(11) to a person whose only use of such information will be in connection with the marketing of a product or service, provided that:

(1) no medical-record information, privileged information, or personal information relating to an individual's health, character, personal habits, mode of living or general reputation is disclosed, and no classification derived from such information is disclosed;

(2) the individual has been given an opportunity to indicate that he does not want personal information disclosed for marketing purposes and has given no indication that he does not want the information disclosed; and

(3) the person receiveing such information agrees not to use it except in connection with the marketing of a product or service or

(12) to an affiliate whose only use of the information will be in connection with an audit of the insurance institution or insurance representative or the marketing of an insurance product or service; provided, however, that the affiliate agrees not to disclose the information for any other purpose or to unaffiliated persons; or

(13) **by** a consumer reporting agency; provided, however, that the disclosure is to a person other than an insurance institution or insurance representative: or

(14) to a group policyholder for the purpose of reporting claims experience or conducting an audit of the insurance institution's or insurance representative's operations or services; provided, however, that the information disclosed is reasonably necessary for the group policyholder to conduct the review or audit; or

(15) to a professional peer review organization for the purpose of reviewing the service or conduct of a medical-care institution or medical professional; or

(16) to a governmental authority for the purpose of determining the individual's eligibility for health benefits for which the governmental authority may be liable; or

(17) to a certificate holder or policyholder for the purpose of providing information regarding the status of an insurance transaction; or

(18) to a lienholder, mortgagee, assignee, lessor or other person shown on the records of an insurance institution or insurance representative as having a legal or beneficial interest in a policy of insurance; provided, however, that:

(i) no medical-record information is disclosed unless the disclosure would otherwise be permitted by this section; and

(ii) the information disclosed is limited to that which is reasonably necessary to permit such person to protect its interests in such policy.

Added by St.1991, c. 516, 9 1

Historical and Statutory Notes

1991 Legislation

Section 2 of St.1991, c. 516, as amended by' St.1992, c. 286, $ 276, provides:

"Chapter 516 of the acts of 1991 is hereby amended by striking out section 2 and inserting in place thereof the following section:—

"Section 2. The provisions of sections eight, nine and thirteen of chapter one hundred and seventy-five I of the General Laws, inserted by section one of this act, shall apply to rights granted therein regardless of the date of collection or receipt of the information which is the subject of such sections. '

St.1992 c. 286, $ 276, an emergency act, was approved Dec. 23, 1992.

14. Investigations

(a) The commissioner shall have power to examine and investigate into the affairs of every insurance institution or insurance representative doing business in the commonwealth to determine whether such insurance institution or insurance representative has been or is engaged in any conduct in violation of this chapter.

(b) The commissioner shall have the power to examine and investigate into the affairs of every insurance-support organization acting on behalf of an insurance institution or insurance representative which either transacts business in the commonwealth or transacts business outside the commonwealth that has an effect on a person residing in the commonwealth in order to determine whether such insurance-support organization has been or is engaged in any conduct in violation of this chapter.

Added by St.1991, c. 516, 1,

15. Violations; notice; hearings; service of process

(a) Whenever the commissioner has reason to believe that an insurance institution, insurance representative or insurance-support organization has been or is engaged in conduct in the commonwealth which violates this chapter, or if the commissioner believes that an insurance-support organization has been or is engaged in conduct outside the commonwealth which has an effect on a person residing in the commonwealth and which violates this chapter, the commissioner shall issue and serve upon such insurance institution, insurance representative or insurance-support organization a statement of charges and notice of hearing to be held at a time and place fixed in the notice, the date of such hearing shall be not less than twenty -one business days after the date of service.

(b) At the time and place fixed for such hearing the *insurance* institution, insurance representative or insurance-support organization charged shall have an opportunity to

answer the charges against it and present evidence on its behalf. Upon good cause shown, the commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person,

(c) At any hearing conducted pursuant to this section the commissioner may administer oaths, examine and cross-examine witnesses and receive oral and documentary evidence. The commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents which are relevant to the hearing. A stenographic record of the hearing shall be made upon the request of any party or at the discretion of the commissioner. If no stenographic record is made and if judicial review is sought, the commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of the commonwealth.

(d) Statements of charges, notices, orders and other processes of the commissioner under this chapter may be served by anyone duly authorized to act on behalf of the commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered mail. A copy of the statement of charges, notice, order or other process shall be provided to the person or persons whose rights under this chapter have been allegedly violated. A verified return setting forth the manner of service, or return postcard receipt in the case of registered mail, shall be sufficient proof of service.

Added by St.1991, c. 516, $ 1

16. Agent for service of process

For the purpose of this chapter, an insurance-support organization transacting business outside the commonwealth which has an effect on a person residing in the commonwealth shall be deemed to have appointed the commissioner to accept service of process on its behalf; provided, however, that the commissioner causes a copy of such service to be mailed forthwith by registered mail to the insurance-support organization at its last known principal place of business. The return postcard receipt for such mailing shall be sufficient proof that the same was properly mailed by the commissioner.

Added by St.1991, c. 516, $ 1.

17. Findings; orders to cease and desist; reports

(a) If, after a hearing pursuant to section fifteen, the commissioner finds that the insurance institution, insurance representative or insurance-support organization charged has engaged in conduct or practices in violation of this chapter, the commissioner shall put such findings in writing and shall issue and cause to be served upon such insurance institution, insurance representative or insurance-support organization a copy of such findings and an order requiring such insurance institution, insurance representative or insurance-support organization to cease and desist from the conduct or practices constituting a violation of this chapter.

(b) If, after a hearing pursuant to section fifteen, the commissioner determines that the insurance institution, insurance representative or insurance-support organization charged has not engaged in conduct or practices in violation of this chapter, the commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the insurance institution, insurance representative or insurance-support organization charged and upon the person or persons, if any, whose rights under this chapter were allegedly violated.

(c) Until the expiration of the time allowed under section nineteen for filing a petition for review or until such petition is actually filed, whichever occurs first, the commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed under section nineteen for filing a petition for review, if no such petition has been duly filed, the commissioner may, after notice and opportunity for **hearing,** alter modify or set aside, in whole or in part, any order or report issued under

this section whenever conditions of fact or law warrant such action or if the public interest so requires.

Added by St.1991, c. 516, $ 1.

$ 18. Penalties; violations **of cease and desist orders**

(a) In any case where a hearing pursuant to section fifteen results in the findings of a knowing violation of this chapter, the commissioner may, in addition to the issuance of a cease and desist order as prescribed in section seventeen, order payment of a monetary penalty of not more than one thousand dollars for each such violation; provided, however, that:

(1) in a hearing to which an insurance representative is a party, the monetary penalty imposed against such insurance representative shall not exceed ten thousand dollars in the aggregate for multiple violations; and

(2) in a hearing to which an insurance institution or insurance-support organization is a party, the monetary penalty imposed against such insurance institution or insurance-support organization shall not exceed fifth thousand dollars in the aggregate for multiple violations.

(b) Any person who violates a cease and desist order of the commissioner under section seventeen may, after notice and hearing and upon order of commissioner, be subject to one or more of the following penalties, at the discretion of the commissioner:

(1) a monetary fine of not more than ten thousand dollars for each such violation;

(2) a monetary fine of not more than fifth thousand dollars if the commissioner finds that such violation has occurred with such frequency as to constitute a general business practice; or

(3) suspension or revocation of an insurance institution's or insurance representative's license.

Added by St.1991, c. 516, $ 1.

19. Judicial review; filing deadline; jurisdiction; orders

(a) Any person subject to an order of the commissioner under section seventeen or section eighteen or any person whose rights under- this chapter were allegedly violated may obtain a review" of any order or report of the commissioner by filing in the supreme judicial court, within twenty days from the date of the service of such order or report, a written petition requesting that the order or report of the commissioner be set aside. A copy of such petition shall be simultaneously served upon the commissioner, who shall forthwith certify and file in such court a transcript of the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and transcript, the supreme judicial court shall have jurisdiction to make and enter a decree modifying, affirming or revcrsing order or report of the commissioner, in whole or in part. The findings of the commisioner as to the facts supporting any order or report, if supported by clear and convincing evdence, shall be conclusive.

(b) To the extent an order or report of the commissioner is affirmed, the court shall issue its own order commanding obedience to the terms of the order or report of the commissioner. If any party affected by an order or report of the commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the commisioner in such manner and upon **such** terms and conditions as the court may deem proper. The commissioner modify his findings of fact or make new findings by reason of the additional eveidence so taken and shall file modified or new findings along with any recommendation, if any for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new' findings shall bc, conclusive as to the matters contained the rein

(c) An order or report issued by the commissioner under sections seventeen or eighteen shall become final:

(1) upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the commissioner may modify or set aside an order or report to the extent provided in subsection (c) of section seventeen; or

(2) upon a final decision of the supreme judicial court if the court directs that the order or report of the commissioner be affirmed or the petition for review dismissed.

(d) No order or report of the commissioner under this chapter or order of a court to enforce the same shall in any way relieve or absolve any person affected by such order or report from any liability under any law of the commonwealth.

Added by St.1991, c. 516, $ 1,

$ 20. Equitable relief; damages; costs and attorney's fees; limitation of actions

(a) If any insurance institution, insurance representative or insurance-support organization fails to comply with sections eight, nine or ten with respect to the rights granted under said sections, any person whose rights are violated may apply to the superior court, or any other court of competent jurisdiction, for appropriate equitable relief.

(b) "An insurance institution, insurance representative or insurance-support organization which discloses information in violation of section thirteen shall be liable for special and compensatory damages sustained by the individual to whom the information relates.

(c) In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.

(d) An action under this section must be brought within two years from the date the alleged violation is or should have been discovered.

(e) Except as specifically provided in this section, there shall be no remedy or recovery available to an individual, in law or in equity, for an occurrence constituting a violation of any provisions of this chapter.

Added by St.1991, c. 516, $ 1.

Q 21. Disclosure of information; immunity

No **cause** of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this chapter; provided, however, this section shall provide no immunity:

(1) for any person who discloses false information with malice or willful intent to injure any person; or

(2) for any person who misidentifies an individual as the subject of information and who discloses such misidentified information to others.

Added by St.1991, c. 516, $ 1.

$ 22. Information obtained by false pretenses; penalties

Any 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 ten thousand dollars or imprisoned for not more than one year, or both such fine and imprisonment.

Added b]' St.1991, c. 516, $ 1

ETHICAL TENETS FOR PROTECTION OF CONFIDENTIAL CLINICAL DATA

Drafted by: Elmer R. Gabrie!i, M.D.
Chief Scientist
Gabrieli Medical *lnformation Systems, Inc.*
Buflalo, New York

PREAMBLE

1. **Right to** privacy is an inalienable right of every American citizen.
2. Patients must have the freedom to fully disclose confidential information to their physicians.
3. It is the traditional duty of the physician to protect the confidential clinical information.
4. Computer technology has altered the risk of unauthorized access to privileged information. Access is virtually invisible.
5. Usc of computers in medicine creates an additional moral obligation.
6. The following ethical tenets concerning computcr-bascd confidcntial patient data delineate the moral commitments. These should be reinforced by statutory laws and intensive education of healthcarc providers and the patient community. Explicit operational standards should further enforce the intent of the tenets and the spirit of the law.
7. When an ethical tenet is written with "shall" as the verb, disciplinary rules must complement the tenc~ and operational standards must reflect the mandatory nature of the tcne~

ETHICAL TENETS

I. ADEQUATE DOCUMENTATION IS AN ESSENTIAL PART OF PRIMARY RECORD SHALL FULLY DOCUMENT THE CARE RENDERED.

"Adequate documetation" means sufficient significant data so that Thc reader of the documentation can understand the clinical situation, the diagnostic conclusion and the therapeutic regimen.

'Esscntial part" means that clinical care and documentation shall be two in.separable components of patient management.

"tire Primary record" means the documetation describing the clinical condition and the care intervention.

"Full document" means to cover the pertinent facts of past clinical history, current status, clin]c:il decisions and efforts to Improvc the physical/mcntal health of Ihc patient.

IL CLINICAL INFORMATION, REVEALED VERBALLY OR RECORDED IN THE PRIMARY CLINICAL RECORD SHALL BE KEPT IN STRICT CONFIDENCE.

"**Clinical information**" is used here in its broadest sense, to include all relevant clinical and socio-economic data disclosed by the patient and others, as we1l as observations, findings, therapeutic interventions and prognostic statements gemerated by the membcrs of the halthcarc team.

"Kept in strict confidencc" means not delibcratcly sharing any part of the clinical information with anyone without explicit permission by the patient/guardian, and that the physician is responsible for guarding the primary clinical record from any unauthorized access. Electronic patient records arc often remote from the physician's sphere of power to control access, but the responsibilit y is not ceascd, only changed. Thccomputcr-based patient record system shall provide the physician with adequate warranty that the clinical data will be securely guarded from unauthorized access.

m. THE PATIENT SHALL BE THE OWNER OF THE IDENTIFIABLE INFORMATION PROVIDED DURING THE COURSE OF THE MEDICAL CARE AS WELL AS OF THE CLINICAL DATA GENERATED IN CONNECTION WITH THE CLINICAL CARE.

Owner neans that the patient,or his legal guardian, alone, has the ultimate total control over the storage, access and change of the identified primary clinical record, and as the owner controls his properties.

"Identifiable information''mcans information linked to personal identifiers such as name, social security number, address, telephonc number, workplace, and other identifiers which may facilitate the identification of the patient.

"Information provided during the course of the medical care" covers [he information volunteered by the patient, by the patient's family, or by his environment.

"During the course of the medical care" intends to li m it the ownership to the information that was disclosed by the patient during the medical examination, discus

sion of the case **management, and** therapy givcn.

"Clincal data generated in connecti"n with the clinical care" refcrs to the diagnostic study results, **consultation reports** and similar subrecords, but does not include the secondary records.

I.V. THE PHYSICIAN SHALL BE THE OWNER OF THE INFORMATION GENERATED BY HIM DURING MEDICAL CARE.

"Physician" in this context includes the physician and mcmbcrs of the healthcarc team.

"Owner the full moral right to privacy and full control of access. Ownership covers the information only, not the information carrying media such as paper, dictation tape or electronic storage media.

"Information generated " represents the diagnostic/ therapeutic / prognostic comments/opinions, decision explanation and choice rationale, i.e., all parts of the clinical reasoning and the pro-fessional interpretation of the data collected. These parts of the primary record are often essential for effective intraprofessional communication and for assessment of the quality of care. The physician's right to professional privacy should be fully protected, to encourage candid recording of the physician's thoughts, suspicions, concerns.

After due consideration and negotiations, other professionals **such as** dent.i.sts, social workers, nurses, and others may wish to be included as professional contributors to the primary clinical records and expect equal protection from unauthorized protection.

V. PRIMARY PATIENT RECORD SHALL BE HANDLED ONLY BY THE PHYSICIAN OR HIS DESIGNEE,

Primary patient record in this context, covers both manual records, kept in the medical records department of the hospital or in the physicians' offices, and automated medical records kept at data centers.

The term "designee" includes the medical record officer(s) (hospital) and office nurse (private office) in the case of manual records, and/or the entireprofessional and non-professional st aff at the data centers, in case of automated patient records.

"Handled", in this context, means collecting, storing, checking, guarding from unauthorized access, and retrieving when appropriate,

VI. PATIENTS SHALL BE KEPT INFORMED OF THE LOCATION, OPERATIONAL PRACTICES AND INFORMATION ACCESS POLICIES OF ELECTRONIC DATA CENTERS.

"Patients" means the entire population of the counmy. "Kcpt informed" means explicit description and explaination of the record storage and access rules and exceptions, as defined in the operational standards of the data centers. These rules and exceptions must be reviewed and approved by the appropriate rcgu-latory organizations.

The data storage/access policies should explain to the patient community the basic rule that the patient is the owner of his own records, and describe the exceptions **such as** regulatory agency functions, or in case of emergency the authorization of the data center'security officer to release key data to the attending physician. Special authorization procedures shall also redescribed such as to legitimate researchers seeking identified clinical information.

WI. THE PRIMARY DUTY OF CLINICAL DATA CENTERS STORING PATIENT RECORDS SHALL BE TO PROVIDE COMPREHENSIVE DATA, IN A TIMELY FASHION, UPON LEGITIMATE DEMAND, TO ASSIST PATIENT CARE MANAGEMENT AND TO PROMOTE PROGRESS IN CLINICAL MEDICINE.

"Primarv dutv''meansthat thedatacentm shall be fully committed to serve the medical data needs. Failure to retrieve requested data should be viewed as breaking a contractual relationship.

"Provideco mmehensivc ~" means to present all the relevant dam in storage, on the patient.

"In timely fashion' 'means that the data release shall not delay the clinical decisions and intawentions. Ergo, "timely fashion" means the most expeditious data release current technology permits.

"Upon legitimate demand" means a care provider, authorized by the patient to request the clinical records, with proof for the purpose for which the records have been requested. The legitimate demand includes mainly the request by a care provider with the intent to render medical care, but it also includes information for quality of care (peer review), teaching andresareh. The legitimate demand shall justify the need for release of the socio-demographic patient identifiers, and the assurance that the recipient of the released data will have the authority and necessary resources for protecting the released data fromunauthorized access by unauthorized persons.

"To assist patient care managment''means that the data release should include; all the data that may help the clinical care provider in the decision making process. This means not only the patient-authorized records, but also algorithmic retrieval of similar cases, as statistical aggregates, to show the prevailing care management process, alternativcs, expected cost outcome, and related benefits.

"Promote progress in medicine" means the responsibility of data centers storing clinical data to continuously monitor the climicat database, derivestatistical inferences, and keep clinical medicine informed about prevalence and occurrence of various clinical conditions, efficicnc y of diagnostic strategics, relative cffec -

tivcncss of various therapeutic choices and long-range outcomcs.

"Paticnt care management means prima facie obligation to assist health delivery, and indirect responsibility for other legitimate users such as teaching, research, administraTivc and fiscal data uses,

VIII. CLINICAL DATA CENTERS STORING PATIENT RECORDS SHALL MAINTAIN APPROPRIATEOPERATIONAL STANDARDS AND RELIABLE DATA SECURITY POLICIFS.

"Clinical data CENTERS means all computer-based systems dealing with patient records, ranging from a solo PRACTITIONERS office computer to large hospital-based data centers and regional data systems, if these data centers regularly store patient records.

"Operational standards" means comprehensive and detailed spcci-fications for data input, storage, processing and disclosure, formal documentation of all personnel policies, employceeducation, gricvanccprocedures, and organizational structure. These operational standards shall be critically reviewed by the overseeing authorities. The clinical data centers shall undergo periodic inspection, monitoring of the effectiveness of the data security system, and evidence for positive attitude of the employees toward the patients' right to confidentiality and the hcalthcare provider's right to privacy.

The clinical data centers shall undergo an initial accreditation process, and periodic renewal of accreditation as a visible method of external control, but, in addition, a stringent internal control system is mandatory, conducted by the supervising group of the data center. Both the external and the in-house control groups shall represent the interests of the patient and the care providers. The regulatory agency shall vigorously examine the clinical data centcr's operating practices, the adequacy and reliability of the hardware, dependability of the applied data security measures, safety and security of storage, effectiveness of processing, and competence of the personnel carrying out the intended functions. The findings of the accrediting agency shall be promptly reviewed by the supervisors of the clinical data center the recommended corrections shall be expeditiously instituted, and the accrediting agency notified about the corrections. Only currently full y accredited clinical data centers should store/retrieve patient records.

Ix. IDENTIFIED SECONDARY CLINICAL RECORDS SHALL RECEIVE CONFIDENTIAL TREATMENT.

"Secondary clinical records" arc the data derived from the primary paticnt record for administative, li.seal, epidemiologic and other similar purposes. Secondary records arc created for a limitcd purpose, arc not a part of the treatment, and not a part of professional communication to contribute to the care of the patient. A rcport by a physician employed by an insu~mpan~r to assess a disability, is a Sccondar, record.

"Identified secondary record" refers to the unique patient identifiers such as name, address, telphone number, or Social Se-curity number. "Identified secondary record" also refers [o unique identifiers of the care providing physician, hcalthcarc team and institution, entitled to right to privacy.

X. IDENTIFIED SECONDARY HEALTH-CARE-RELATED RECORDS SHALL BE USED ONLY FOR THE ORIGINAL PURPOSE FOR WHICH THEY WERE GENERATED, AND SHALL BE DESTROYED, OR AT LEAST MISIDENTIFIED, A S PROMPTLY AS POSSIBLE.

" scd Used only for the orginal porpose for which they were generated limits the use of secondary medical information for the sole purpse forwhich the record was requested. For example, it would be unethical to usc a psychiatric registry for comparison with the list of applicants for gun license, or to find drug users. The patient's right to confidentiality would be violated if medical information shared in an atmosphere of apparent confidence would be used for law enforcement or other non-medical purposes.

"Destroyed" means physical destruction of a paper document or purging an electronic database to remove the data once the task is accomplished. For instance, third party carries should destroy the claims, once the fiscal transaction is completed. For actuarial purposes, disidentified data could be used, when feasible.

Release of any aggregate data derived from primary or secondary medical records, such as research reports shall be in such form as not to permit the identification of any persons whose identified records were utilized in the research. It shall be the responsibility of the researcher to ensure that these conditions are met. If for public health or research purposes, any release of identified secondary information shall be desirable or appropriate, the informed consent and explicit formal authorization of the patient or his guardian shall be sought and attained prior to such release. Release of identified primary or secondary patient records to a researcher who is not a part of the patient's healthcarc team shall, of course, also require the informed consent and explicit formal authorization of the patient or his guardian.

XI. FACH DATA CENTER HANDLING IDENTIFIED MEDICAL DATA SHALL EXPLICITLY DEFINE ITS SPECIFIC COALS. THESE GOALS SHALL BE MORALLY CONSISTENT AND COMPATIBLE.

"Data ccntcr" means the entire ensemble of people who have access to the data, including those at the data gcncration site, transmission to the data centcr, and all those who work directly with a computer-bawd mcdical

information handling system and those who provide data for such an information system, The same rules shall apply also to those who participate in manual handling of medical information. In the hospital, the medical records department shall be responsible for the identification of all the groups, offices and individuals who provide data for any type of computerization, ranging from utilization reports to business office and to quality assurancc groups. Such a study should be summarized in the form of a data security report The report should be reviewed by the (medical) executive committee of the hospital and filed with their minutes. Another copy should be scrutinize by the hospital administrator and the advisory board, and after approval, a copy of this document should be kept on file. Any change in data release practices in the hospital should be formally recognized, and copies of the report should be filed with the above two groups (medical executive committee and advisory board).

Particular attcntion should be devoted to the process of data transfer. In some hospitals commercial telecommunication systems arc used for data transfer. The hospital is also responsible for the selection of the data security criteria and for supervision of the operation of such an intermediary telecommunication system.

Thus the term "data center''covers the entire path of data flow, from the paticnt to the computer opcration and includes the data providers, data processor, and data users.

"Handling"means bothphysical access forproccssing and storage and dissemination.

"Handling identified medical data" means all those who handle the medical data or who may have access to such data during thecourscof their work such as cleaning personnel.

"Identificd **medical data" means any** combination of a patient identifier and a clinical datum. The patient identifier may be direct and unique such as name, or address, or Social Securitynumber, orless specific such as date of hospitalization with record number or birth date, or implicit such as the data person's social identified, insurance numbers. The term "Identified medical data'' shall be interpretedbroadly since even nonspecific implicit idcntificxs maybe used to "track down" a data person. This is a rather simple procedure. It is possible to combine the medical data listing with another listing. For example, in a community databank, an explicit list of the population may be combined with medical data listing which may fully identify the data person.

"Medical data" includes both the primary and the secondary medical records as defined in the Ethical Guidelines.

"Shall means a moral legal imperative. Violation means punitive measure.

"Explicity define''mc.ansa formal document drafted specifically to define the goals.

"Specific goals" of a data centcr arc the formally and explicitly defined purposes for medical data collcc**tion, processing, storage and dissemination. The** borders of these specific goals shall be sharply defined. For example, if the data centcr's only goal is to process reimbursement claims for an insurance carrier, this goal must & sharply defined, excluding all other related.cd functions such as actuarial studies, diseases registries or patient history files. After the initial definition of the specific goals, any subsequent change in goals shall require formal amendment of the original document stating the reason(s) and the extent of the change and/or the exact expansion of the initial goal. In most general terms, the definition of the specific goals also justifies the collection of medical data. The goal maybe support of medical care, necesary administrative managerial, an epidemiologic study, fiscal processing of claims, monitoring of the quality or appropriateness of medical care, drug evaluation or follow-up of a therapeutic procedurc. It is possible that a data center collects medical data for more than one goal, such as the recently created state-wide governmental data centers. In such cases, each goal shall be defined separately, with justification of each goal.

"Morrally **means that the data** center shall honor the moral principles of the Ehical Guidclincsand therefore, morally conflicting goals shall not be combined. As a simple rule, medical goals should not be combined with non-medical goals. For example, a psychiatric registry should be justified only for medical poposes such as the study of the natural course of [illegible] or evaluation of the effectiveness of various drugs. The same psychiatric registry shall not be used for non-medical purposes such as gun license control, legal or criminal evidence gathering. If a data center's stated goal is fiscal processing or reimbursement claims, the same database should not be used for evaluation of quality of care. 'Those who pay for servises should not judge these services since such a combination would be a conflict of interests. (Similar combination of conflicting functions in the legal branches would be equally objectionable.) Based on the same reasoning, if the goal of a data center is administrative, such as a govcrnmental data system, it should not be combined with madical or fiscal purposes such as public health or insurance fraud. The chosen goals of a medical data center shall not be selfserving or possible leading to any conflict of interests. The three branches of the health industry should remain sharply separated. These arc: (1) Medical purposes, (2) Fiscal purposes, (3) Administrative monitoring purposcs.

"Compatible" means that in case of multiple goals these should be synergistic toward the stated purpose.

The intent of this rule is to encourage the development of dedicated medical data centers with highly visible purpose.

XII. EACH DATA CENTER HANDLING IDENTIFIED MEDICAL DATA SHALL FORMULATE AND MAINTAIN ITS OWN OPERATIONAL RULES AND PRACTICE.'.

"Formulate" means a writtcn, formal and comprehensive document describing the data center's opcrational rules and practices. This documcnt should be known to all employecs, and all those who deal with the data center.

"Maintain" means a continuous running account of the prevailing rules and prioritics, with regular updaing as wel as periodic rc-evaluation of the document containing the operational rules and practices. proper maintenance of this fundamental document shall keep the documcnt currcnt

"Opcrational rules and practices" means explicit description of the staffing, authority rules, general polices, specific regulations defining data acquisition, storage, access, right to modify, right to process and rules of dissenubation and releasc of identifiable medical information. Thc operational rules shall coverall aspects of the operation of the data centcr.

The intent of this rule is to encourage a highly structured and formalizcd operation when dealing with sensitive medical data.

XIII. THE CHOSEN GOALS AND THE OPERATIONAL RULES AND PRACTICES SHALL BE FORMALLY ENDORSED BY THE OPERATIVE AUTHORITIES AND BY THE PROVIDERS OF THE MEDICAL DATA. THE AUTHORIZED GOALS AND OPERATIONAL RULES AND PRACTICES SHALL BE MADE PUBLIC AND AVAILABLE TO ALL DATA PERSONS.

"Chos e "refccs to the documcntdcfined in the eleventh rule of this ocumcn~

'Opcrational rules and practices "refers to thedocumcnt defined in the twelfth rule of this guideline. These two documcnts constitute the charter of the medical data center.

"formallv endorsed" means that the medical data center's charter shall be reviewed, accepted and formally approved, after due process, and according to the organization's own hierarchical structure, constitution and by~~laws.

61 Opcative authoritie " means all those who may, organizationally and/or fiscally, control the data center. In a hospital, these operative authorities may include the hospital administration, the board of directors and the cxecutivc committee of the medical staff. In a state health department, the operative authorities may include (a) the health commissioner, (b) the legislators (assembly and senate) and (c) the governor's office.

In the health/life insurance indus, this may include the members of thc board, officers, administrators and local managcrsof any stock company, mutual funds, BlucCrossor Blue Shield type organizations and administrators of any govcrnment plan or law, and also those who have thc right to appoint or promote the director and the staff mcmbcrs and/or those Who may affect he budget of the data systemq. Thus the charter of a medical centcr must be recognized, endorsed and fully respected by the supporting organization.

"Providers of medical data" means only the physicians and all other members of the healthcare providing team who had generated the medical information which is subsequently handled by the data center. Thus the ultimate responsible party is the person who generates the medical data and is directly responsible to the patients. Provider o f medical data' 'cannot be a hospital or a clinic clerk. The medical data generator shall be directly rcsponsiblc for the adequacy of the charter.

"Made public" means making it readily available to any justifiably interested person.

"Available to all data persons" means all those individuals (patients) about whom any identified or identifiable data are kept and/or processed by the data ccntcr.

The intent of this rule is to achieve full endorsement and ac-ceptance of the charter by the entire organization which may exert any pressure on the data center for access or releasc of any data. This rule intends to protect the data center from external influences so that the full and undivided responsibility is con-centrated in the hands of the leaders of the data center. Clinical medicine must be fully aware of the charter of the data center in order to assess the implicit risks of data generation/ release. Thus the charter shall be a carefully drafted, highly visible document the moral foundation of the medical data center.

XIV. EACH MEDICAL DATA CENTER SHALL FORMULATE 113 OWN EXPLICIT PERSONNELPOLICIES IN REGARD TO CONFIDENTIALITYAND PERSONNEL INTEGRITY AND SHALL DESCRIBE THESE POLICIES INTHEOPERATIONAL RULES AND PRACTICES.

"Formulate its own e~xdicit personncl policicS" means detailed job descriptions, succinct definition of rights and responsible of each job, including, but not limited to:

- education requirements,
- required job experience,
- extent of required formal training in medical ethics.

The document shall cover hiring practices and gathering of various types of references.

A copy of the current records of the personnel shall be kept in a file accessible to the accrediting agency.

Before hiring the candidate shall review charter, fully understand the data center's purpose and operational rules and sign an agreement to honor the charter of the data systcm.

Any violation of an ethical rule shall lead to invcstigation and dismaissal by duc process, and with formal

notification of the accrediting agency so that a list of dismissed people is available [o data centers, upon authorized inquiry.

The personnel policies shall require regular "in-serviice" meetings with mandatory attendance by the personnel of the data center. These in-service meetings should focus on medical ethics as it relates to the patient's inalienable right to privacy. These in-service meetings shall be integrated with periodic attendance of national meetings concerned with some ethical aspects of medical information processing. The participants of in-service meetings and national meetings shall keep detailed records of these meetings. Organized efforts shall be made to make (and keep) the personnel of the data center constantl y aware of the absolute necessity of ethical behavior and moral integrity, not only at the job, but encompassing their entire personal life. The general rules shall be similar to those adopted by organizations protecting classified military information.

The medical data center shall maintain a general model of ethical guidelines specifically drafted for data center directors, systems analysts, programmers, machine operators, clerical employees, and in particular for data security officers.

The intent of this rule is to explicate the necessary sclfimposed (voluntary) self-control and professionalism for the staff of the data center which is traditional in clinical medicine, nursing and allied health professions. Since the medical data center is a newcomer to clinical medicine, this rule intends to transfer the prevailing attitudc of the hcalthcarc providers to the ncwcomcr, the staff of the data center.

XV. EACH MEDICAL DATA CENTER SHALL DEVELOP AND MAINTAIN A CONTROL RECORD ON ALL MEDICAL DATA IN THE DATABASE.

"Develop" means an explicit description of the types of potentially sensitive data collected / stored / processed /released. Thesc data shall be fully characterized covering origin, structure, and format. Thus the first part of the CONTROL RECORD is the- of all the sensittive data types with adequate characterization of each of the data types.

"Maintain" means continuous updating of the Medical Data Control Record, to keep it current and accurate. Any discrepancy between the Data Control Record and the database would indicated either negligence or deliberate misinformation of the accrediting agency.

The Control Record of Medical Data shall enumerate each data type collected, stored, processed and released by the data center. In addition to cataloging the Control Record shall keep a detailed dcscription of the fate of the data type once it is generated by the healthcarc provider such as the physician, nurse or mcdical record administrator. The minimum list of information to be kept is:

- **the** name of thc **datum** (such as first discharge diagnosis, or surgery performed);
- definition of the datum focusing on the generation and circumstances of recording at the site of patient care;
- dcscriptionof generator who lcnds a definable authority to the datum;
- codc(s) applied to transform the narrative natural language datum into machine-compatible symbols; this segment requires also the filing of the code scheme if the codes arc by local authority;
- method of coding such as manual or automated; if manual the coder shall be identified;
- data field characteristics and typical data structure;
- level of accuracy and reliabilitv of each datum;
- of the datum after entry: storage, address, data protection attached (access rules);
- authorized use of the datum and legitimate recciver(s) of the datum, identified and disidcntified, protection of data integrity;
- owncr of the datum, right to edit, moral obligation to the data person:
- risk value; Level of sensitivity and danger of accidental or malicious access:
- mode and duration of storage; - any other pertinent information such as date of beginning of collection, typical volume at any time, relationship to the goal of the data center, etc.

The intent of this rule is to demand formal documcntation of the database, collection, access and storage. This Data Control Record shall be an essential document for external audit and accreditation.

XVI. EACH DATA CENTER SHALL DEVELOP AND MAINTAIN A DIRECTORY OF DATA USERS.

"Develop" means construction of a formal listing. The director is responsible for the construction and Completeness of this list. No identified or misidentified data should be released or persons or organizations not listed on the users' directory.

"Maintain" means continuous updating in order to keep the **users'** directory **current**

"Directory "meansa comprehensive tabulation with each user's name, address, telephone number, exact description of the user's position and background, the right-to-see aspects, specific level of authorization and method of data protection at the user's site. If identified medical data arc released to a user, the data center remains responsible for the supervision of data security at the user's site.

"Data user" is a person, or an institution/agency receiving directly or indirectly, regularly or occasionally, identifiable medical data, formally defined by the data center.

The dcscription of specific authorization for each user shall explicitly state the type of data for which the authorization has been issued, as wc1l as the amount of formal orientation provided concerning the ethical rc-sponsibilitics of the data uscr, the outlinc of the process of physical disposition of all hardcopy rcports after their use, or the local proteivc measures for storage of lhcsc hard copy reports.

The ntcntof this rule is to describcthc authorizaion process and to explicitly state the responsibility of the data processing ccntcr for the data rcleascd. The users must be defined in the charter, in general, and in the users' directory in particular.

XVII. THE SCOPE OF DATA COLLECTION AND THE EXTENT OF DATA PROCESSING MUST BE EXPLICIT AND LIMITED TO THE STATED GOAL OF TIIE DATA CENTER.

Scope of data collection "on" is thc collective term for all identified medical information entered into the information system, as well as all the non-medical data gathered.

"Extcnt of data processing" is the dcfinition of the series of steps in routine information processing.

"Explicit" *means* clear and specific delineation of the scope of data collection and the extent of data processing.

"Limite to the stated goals" means that every data processing step shall be justifible and explainable as a necessary step for achieving the objectives of the data system, as stated in the charter.

The intent of this rule is to prevent collection of any data not obviously needed for the stated goals and to prevent data processing beyond the stated goals. For example, to an administrator it may seem useful and economical to link a patient's medical data to his school records, criminal records, or tax records. This may assist the educational authorities, police, or IRS. However, from amoral point of view, any such file linkage, unless it is stated in thc goals, would bean abuse of medical data processing. File matching shall not be permited without its description in the charter and **without written con.sent** of the data person(s) or their representative and by the data generator(s), as well as after written consent by the accrediting agency. The staff of the information system shall be acutely aware of the moral constraints which limit the data handling to the chosen stated goal,

XVIII. ADEQUATE DATA SECURITy' MEASURES SHALL BE DEVISED AND MAINTAINED, TO PROTECT TIIE INTEGRITY AND CONFIDENTIALITY OF IDENTIFIED MEDICAL INFORMATION.

"Adequate data security measures" means that the degree of data security shall be proportional to the risks and to the sensitivity of each medical datum. To achieve this focused **protection the information system shall** develop a specific assessment of the potential risk for each data clement if released to an unauthorized user. This way, the data center shall determine the consequenccs of any errors in terms of inadvcrtcnt loss or alteration of the data, and the potential injury if a confidential datum is accesscd by an unauthorized person. In the planning process, the cost of various data security measures shall be considered in the light of their social damage. Clear documentation shall support the rationale of choosing the actual security measures, listing also all reasonable alternatives.

"Devised" **means a** fully cohesive system of data security **measures.**

"Mainntained" means regular periodic testing of the data security in order to ascertain that both the human and technical aspects of the security system arc kept at the lcvcl selected initiall y by the planners of thes systcm. Periodic internal testing of the security shall be formally documented.

The intent of this rule is to requirc a formally documented data security system as an inseparable part of the Operational Rules and practices in the charter.

XIX. EACH DATA PROCESSING GROUPHANDLING IDENTIFIED MEDICAL DATA SHALL NAME SINGLE INDIVIDUAL TO BE RESPONSIBLE FOR DATA SECURITY.

"Name" means a formal appointment of a person and record this action in the charter.

"Single individual" means a member of the information system's staff throughout the period of operation. 'There shall be another individual substituting during illness or vacations, appointed on a temporary basis by the individual named as the person responsible for security. This also means that a data system shall have a responsible person prcscnt throughout the scheduled operation, and that the data system shall never operate without the presence of the data security person.

"Responsibe" means moral and legal liability. The person re-sponsiblc for the day-to-day control of all data security measures shall be an individual with adequate background in medical records and data processing, and with special formal training in data security measures,. It is not acceptable to appoint a medical record or a data processing person to scrvc as data security officer, unless this person can prove training and experience spccify_-cally **in** the area of data security. This person should hold periodic meetings with the members of the data centcr to discuss data security, and this person should regularll attend national meetings where advances in data protection.

The intent of this rule is to stress that a data security person responsible for sensitive medical data must meet both technical and ethical standards. The latter requires the presence of the person responsible for data security. If the data system's staff is small and it is not practical to separate technical and ethical responsibilities, special

plans shall bc formulated for satisfactory combination of the two functions.

XX. THE DATA SECURITY PERSON SHALL MAINTAIN DAILY RECORD OF EVENTS RELATED TO DATA PROTECTION. THIS DAILY RECORD SHALL BE ACCESSIBLE TO ACCREDITING AGENCIES

"Data security person" is the formally appointed person as defined in the nineteenth rule.

"Maintain" means keeping the record on a day-to-day basis.

"Events related to data protection" includes all hardware problems, programming events and routine procedures which may have an impact temporary or permanent, on the formal data security program. For example, a hardware failure requiring repeat collection or entry of data, or a request by a user different from established routine, shall be recorded on a day-today basis. In emergency situations, the data security person shall be the only authorized person to release data which deemed justified, but a retroactive authorization will be necessary following such an event

"Accessible to accrediting agencies" means that the daily data security record shall be submitted to the accrediting agency, as an important document reflecting the quality of data security. Periodic review of this document by the supporting agency seems appropriate but not mandatory. This decision should be a part of the accrediting process.

The intent of this rule is to formalize the role of the data security person. The daily record is intended to keep those responsible for the data security system vigilant and aware of the importance of the privacy aspects.

XXI. THE DATA AS WELL AS THE DATA PROTECTION PRACTICES SHALL BEAVAILABLE TO THOSE JUSTIFIABLY **REQUESTING INFORMATION ABOUT THEMSELVES**

"Data" means those particular **medical and identifying data which are stored in one data person's file.**

"Dataprotection pratices" **means a copy of the security systems described in the** Chatter.

"Availabe" means access upon regulated requcst.

"Justifiably" means According to the Freedom for Information Act

The intent of this rule is to **provide for access of** information **kcpt on fileb about a data person. Dueproeess shall be devised enabling the data person to request corrcetion when this is due, i.e., when the data person has** provided adequate evidence showing that a particular datum is incorrect. If **the error is due to a data entry error the data center is responsible for the correction, whereas** if the error was at the **site of the data generation, the** health provider **shall modify the datum.**

XXII. THE DATA **CENTER PROCESSING IDENTIFIED MEDICAL DATA SHALL BE LI**ABLE FOR INTEGRITY AND PROTECTION OF THE MEDICAL DATA.

"Liable" means **moral and legal responsibility.**

"Integrity" means the accuracy of the data, exact correspondence with the source document While the hcaltheare provider is responsible for the clinical accuracy of the generated data the data centcr is liable for protection of data integrity, processing without loss, distortion or any **other alteration.**

"Protection" means guarding from unauthorized access.

The intent of this rule is to state the prirmary and direct responsibility of the data center.

Uniform Health Care Information

50-16-501. Short title. This part may be cited as the "(Uniform Health Care Information Act".

History: **En. .Sec. 1. Ch. 632, I.. 1987.**

50-16-502. Legislative findings. The legislature finds that:

(1) health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy and health care or other interests;

(2) patients need access to their own health care information as a matter of fairness, to enable them to make informed decisions about their health care and to correct inaccurate or incomplete information about themselves;

(3) in order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information;

(4) persons other than health care providers obtain, use, and disclose health record information in many different contexts and for many different purposes. It is the public policy of this state that a patient's interest in the proper use and disclosure of his health care information survives even when the information is held by persons other than health care providers.

(5) the movement of patients and their health care information across state lines, access to and exchange of health care information from automated data banks, and the emergence of multistate health care providers creates a compelling need for uniform law, rules, and procedures governing the use and disclosure of health care information.

History: En. Sec. 2, **Ch.** 632, L. 1987.

50-16-503. Uniformity of application and construction. This part must be applied and construed to effectuate their general purpose to make uniform the laws with respect to the treatment of health care information among states enacting them.

1 History: **Eh. Sec. 3, Ch. 632, I. 1987.**

50-16-504. Definitions. As used in this part, unless the context indicates otherwise, the following definitions apply

(1) "Audit" means an assessment, evaluation, determination, or investigation of a health care provider by a person not employed by or affiliated with the provider, to determine compliance with:

(a) statutory, regulatory, fiscal, medical, or scientific standards;

(b) a private or public program of payments to a health care provider: or

(c) requirements for licensing, accreditation, or certification.

(2) "Directory information" means in information disclosting the presence and the general health condition of a patient who is an inpatient in a health care facility or who is receiving emergency' health care in a health care facility.

(3) "General health condition'" means the patient's health status described in terms of critical, poor, fair, good," excellent, or terms denonting similar conditions.

(4) "Health care" means any care, service , or procedure provided by a health care provider, including medical or psychological" diagnosis, treatment,

evaluation, advice, or other services **that** affect the structure or any function of the human body.

(5) "Health care facility" means a hospital, clinic, nursing home, laboratory, office, or similar place where a health care provider provides health care to patients.

(6) "Health care information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and relates to the patient's health care. The term includes any record of disclosures of health care information.

(7) "Health care provider" means a person who is licensed, certified, or otherwise authorized by the laws of this state to provide health care in the ordinary course of business or practice of a profession. The term does not include a person who provides health care solely through the sale or dispensing of drugs or medical devices.

(8) "Institutional review board" means a board, committee, or other group formally designated by an institution or authorized under federal or state law to review, approve the initiation of, or conduct periodic review of research programs to assure the protection of the rights and welfare of human research subjects.

(9) "Maintain", as related to health care information, means to hold, possess, preserve, retain, store, or control that information.

(10) "Patient" means an individual who receives or has received health care. The term includes a deceased individual who has received health care.

(11) "Peer review" means an evaluation of health care services by a committee of a state or local professional organization of health care providers or a committee of medical staff of a licensed health care facility. The committee must be:

(a) authorized by law to evaluate health care services; and

(b) governed by written bylaws approved by the governing board of the health care facility or an organization of health care providers.

(12) "Person" means an individual, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or other legal or commercial entity.

History En. Sec. 4, Ch. 632, 1,. 1987.

Cross-References

Government health care information – defi nition of health care in informat ion, 50-16-602.

50-16-505 through 50-16-510 reserved.

50-16-511. Duty to adopt security safeguards. A health care provider shall effect reasonable safeguards for the security of all health care information it maintains.

H i story: Kin. Sec. 21, (Ch. 632, 1,.1987.

50-16-512. Content and dissemination of notice. (1) A health care provider who provides health care at a health care facility that the provider operates and who maintains a record of a patient's health care information shall create a notice of information practices, in substantially the following form:

NOTICE

"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 . . . . . .

(2) The health care provider shall post a copy of the notice of information practices in a conspicuous place in the health care facility and upon request provide patients or prospective patients with a copy of the notice.

History: En. Sec. 18, Ch. 632, L. 1987.

50-16-513. Retention of record. A health care provider shall maintain a record of existing health care information for at least 1 year following receipt of an authorization to disclose that health care information under 50-16-526 and during the pendency of a request for examination and copying under 50-16-541 or a request for correction or amendment under 50-16-543.

History: En. Sec. 22, Ch. 632, L. 1987.

Cross-References

Records and reports required of health care facilities – confidentiality, 50-5-106.

Maintenance and confidentiality of records concerning develpmentally' disabled persons, ,53-20-161.

50-16-514 through 50-16-520 reserved.

50-16-521. Health care representatives. (1) A person authorized to consent to health care for another may exercise the rights of that person under this part to the extent necessary to effectuate the terms or purposes of the grant of authority. If the patient is a minor and is authorized under 41-1-402 to consent to health care without parental consent, only the minor may exclusively exercise the rights of a patient under this part as to information pertaining to health care to which the minor lawfully consented.

(2) A person authorized to act for a patient shall act in good faith to represent the best interests of the patient.

History: **En. Sec. 19, Ch. 632, L. 1987.**

50-16-522. Representative of deceased patient. A personal representative of a deceased patient may exercise all of the deceased patient's rights under this part, If there is no personal representative or upon discharge of the personal representative, a deceased patient's rights under this part may be exercised by the surviving spouse, a parent, an adult child, an adult sibling, or any other person who is authorized by law to act for him.

History: En. Sec. 20, Ch. 632, L. 1987: amd. Sec. 1, Ch. 657, L. 1989.

Compiler's Comments

1989 Amendment Near end substituted "the surviving spouse, a parent, an adult child, an adult sibling, or any other person" for "persons"; and made minor change in grammar

50-16-523 and 50-16-524 reserved.

50-16-525. Disclosure by health care provider. (1) Except as authorized in 50-16-529 and 50-16-530 or as otherwise specifically provided by law or the Montana Rules of Civil Procedure, a health care provider, an individual

who assists a health care provider in the delivery of health care, or an agent or employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization. A disclosure made under a patient's written authorization must conform to the authorization.

(2) A health care provider shall maintain, in conjunction with a patient's recorded health care information, a record of each person who has received or examined, in whole or in part, the recorded health care information during the preceding 3 years, except for a person who has examined the recorded health care information under 50-16-529(1) or (2). The record of disclosure must include the name, address, and institutional affiliation, if any, of each person receiving or examining the recorded health care information, the date of the receipt or examination, and to the extent practicable a description of the information disclosed.

History: En. Sec. 5, Ch. 632, L. 1987; amd. Sec. 2, Ch. 657, L. 1989.

Compiler's Comments

1989 Amendment Near end of first sentence of (?), after "except for", deleted "an agent or employee of the health care provider or" and after "50- 16-529" inserted "(1) or",

Cross-References

Right of privacy, Art. II, sec. 10, Mont. Const.

Physical and mental examination of persons, Rule 35, M. R. Civ.P. (see Title 25, ch. 20).

Doctor-patient" privilege, 26-1-805.

Privileges, Rules 501 through 505, M. M.R.E (see Title 26, ch. 10).

Gunshot or stab wounds – reporting by' health care practitioners, 37-2-302.

Release of Information by physician (concerning minor, 41-1-403.

Records and reports required of health care facilities – confidentialility}, 50-5-106.

Confidentiality' under 'Tumor Registry} Act, ***50-15-*** **'704.**

Unauthorized divulgence of serological test information, 50-19-108.

Maintenance and confidentiality of records concerning developmentally disabled person, **53-20-161.**

Confidentiality of records concerning mental illness, 53-2 I -166.

Records of chemically dependent persons, intoxicated person, and familly" members, 53-24-306.

50-16-526. Patient authorization to health care provider for disclosure. (1) A patient may authorize a health care provider to disclose the patient's health care information. A health care provider shall honor an authorization and, if requested, provide a copy of the recorded health care information unless the health care provider denies the patient access to health care information under 50-16-542.

(2) A health care provider may charge a reasonable fee, not to exceed his actual cost for providing the health care information, and is not required to honor an authorization until the fee is paid.

(3) To be valid, a disclosure authorization to a health care provider must:

(a) be in writing, dated, and signed by the patient:

(b) identify the nature of the information to be disclosed; and

(c) identify the person to whom the information is to be disclosed.

(4) Except as provided by this part, the signing of an authorization by a patient is not a waiver of any rights a patient has under other statutes, the Montana Rules of Evidence, or common law.

History: En. Sec. 6. Ch. 632. 1.. 1987.

Cross-References

Privileges, Rules 501 through 505, M.R, E\', (we Title 26, ch. 10),

50-16-527. Patient authorization — retention — effective period exception. (1) A health care provider shall retain each authorization or

revocation in conjunction with any health care information from which disclosures are made.

(2) Except for authorizations to provide information to third-party health care payors, an authorization may not permit the release of health care information relating to health care that the patient receives more than 6 months after the authorization was signed.

(3) An authorization in effect on October 1, 1987, remains valid for 30 months after October 1, 1987, unless an earlier date is specified or it is re~'eked under 50- 16-528. Health care information disclosed under such an authorization is otherwise subject to this part, An authorization written after October 1, 1987, becomes invalid after the' expiration date contained in the authorization, which may not exceed 30 months. If the authorization does not contain an expiration date, it expires 6 months after it is signed.

(4) Notwithstanding subsections (2) and (3), a signed claim for workers' compensation or occupational disease benefits authorizes disclosure to the workers' compensation insurer, as defined in 39-71-116, by the health care provider. The disclosure authorized by this subsection relates only to information concerning the claimant's condition. This authorization is effective only as long as the claimant is claiming benefits,

History En. Sec. 7, Ch. 632. 1.. 1987; **amd. Sec. 13, Ch. 333, L, 1989.**

Compiler's Comments

1989, Amendment: Inserted (4) allowing dis-Closure health care in information by health care provider to insurers or in information relating claimant's condition so long as claimant is receiving benefits. Amendment effective March 27, 1989,

Retroactive **applicability: Section** 16, Ch. 333, 1.. 1989, provided that this section applies retroactively, within the meaning of 1-2-109, to all requests for health care information in workers' compensation claims,

50-16-528. Patient's revocation of authorization for disclosure. A patient may revoke a disclosure authorization to a health care provider at any time unless disclosure is required to effectuate payments for health care that has been provided or other substantial action has been taken in reliance on the authorization. A patient may not maintain an action against the health care provider for disclosures made in good-faith reliance on an authorization if the health care provider had no notice of the revocation of the authorization.

History: **Sec. 8, Ch.** 632, L. 1987.

50-16-529. Disclosure without patient's authorization based on need to know. A health care provider may' disclose health care information about a patient without the patient's authorization, to the extent a recipient needs to know the information, if the disclosure is:

(1) to a person who is providing health care to the patient;

(2) to any other person who requires health care information for health care education: to provide planning, quality assurance, peer review, or administrativee, legal, financial, or actuarial services to the health care protvider; for assisting the health care prey'ider in the delivery of health care; or to a third-part] health care payror who requires health care information and if the health care provider reasonably believes that the person will:

(a) not use or disclose the health care information for any other purpose; and

(b) take appropriate steps to protect the health care information;

(3) to any other health care provider who has previously provided health care to the patient, to the extent necessary to provide health care to the patient, unless the patient has instructed the health care provider not to make the disclosure;

(4) to immediate family members of the patient or any other individual with whom the patient is known to have a close personal relationship, if made in accordance with the laws of the state and good medical or other professional practice, unless the patient has instructed the health care provider not to make the disclosure;

(5) to a health care provider who is the successor in interest to the health care provider maintaining the health care information;

(6) for use in a research project that an institutional review board has determined:

(a) is of sufficient importance to outweigh the intrusion into the privacy of the patient that would result from the disclosure;

(b) is impracticable without the use or disclosure of the health care information in individually identifiable form;

(c) contains reasonable safeguards to protect the information from improper disclosure;

(d) contains reasonable safeguards to protect against directly or indirectly identifying any patient in any report of the research project; and

(e) contains procedures to remove or destroy at the earliest opportunity, consistent with the purposes of the project, information that would enable the patient to be identified, unless an institutional review board authorizes retention of identifying information for purposes of another research project;

(i') to a person who obtains information for purposes of an audit, if that person agrees in writing to:

(a) remove or destroy, at the earliest opportunity consistent with the purpose of the audit, information that would enable the patient to be identified; and

(b) not disclose the information further, except to accomplish the auditor to report unlawful or improper conduct involving fraud in payment for health care by a health care provider or patient or other unlawful conduct by a health care provider; and

(8) to an official of a penal or other custodial institution in which the patient is detained.

History **En. Sec. 9, Ch.632, L. 1987; amd. Sec.3, Ch. 657,1. 1989.**

Compiler's Comments

1989 *Amendment* In (2), after "delivery of health care'', inserted "or to at third-partyhealth care payer who requires health care information"; and made minor change in phraseolo.

Cross-References

Duty of mental health professionals To warm of violent patients, 27-1-1102.

Nonviability for peer review, 37-2-201.

Pharmacists not 1 liable for peer review, 37-7-1101.

Release of information by physician concerning minor, 41-1-403.

Maintenance and confidentiality. of records concern i n g developmentally d i sa bled persons, 53-20-161.

Confidentiality of records concerning mental illness, 53-21-166.

50-16-530. Disclosure without patient's authorization — other bases. A health care provider may disclose health care information about a patient without the patient's authorization if the disclosure is:

(1) directory information, unless the patient has instructed the health care provider not to make the disclosure;

(2) to federal, state, or local public health authorities, to the extent the health care provider is required by law to report health care information or when needed to protect the public health;

(3) to federal, state, or local law enforcement authorities to the extent required by law;

(4) to a law enforcement officer about the general physical condition of a patient being treated in a health care facility' if the patient was injured on a public roadway or was injured by the possible criminal act of another;

(5) in response to a request of the division of crime control for information under 53-9-104(2)(b); or

(6) pursuant to compulsory process in accordance with 50-16-535 and 50-16-536.

History **En. Sec. 10, Ch. 632. 1.. 1987: amd. Sec. 1, Ch. 68, L. 1989.**

Compiler's Comments

J989 Admendment Inserted (5) allowing disclosure without patient's authorization of informat ion under The Crime Victims compensation Act of Montana upon request by Division of Crime (Control." Amendment effective March **13,** 1989.

50-16-531 through 50-16-534 reserved.

50-16-535. When health care information available by compulsory process. (1) Health care information may not be disclosed by. a health care provider pursuant to compulsory legal process or discovery in any judicial, legislative, or administrative proceeding unless:

(a) the patient has consented in writing to the release of the health care information in response to compulsory process or a discover}" request;

(b) the patient has waived the right to claim confidentiality for the health care information sought;

(c) the patient is a party to the proceeding and has placed his physical or mental condition in issue;

(d) the patient's physical or mental condition is relevant to the execution or witnessing of a will or other document;

(e) the physical or mental condition of a deceased patient is placed in issue by any person claiming or defending through or as a beneficiary' of the patient;

(f) a patient's health care information is to be used in the patient's commitment proceeding;

(g) the health care information is for use in any law enforcement proceeding or investigation in which a health care provider is the subject or a party, except that health care information so obtained may not be used in any proceeding against the patient unless the matter relates to payment for his health care or unless authorized under subsection (i);

(h) the health care information is relevant to a proceeding brought under 50-16-551 through 50-16-553;

(i) a court has determined that particular health care information is *sub*-ject to compulsory- legal process or discovery because the party seeking the information has demonstrated that there is a compelling state interest that outweighs the patient's privacy' interest; or

(j) the health care information is requested pursuant to an investigative subpoena issued under 46-4-301.

(2)Nothingin this part authorizes the disclosure of health care informati$_{o}$n bycompulsory legal process or discovery in any judicial, legislative, or administrative proceeding where disclosure is otherwise prohibited by law.

History: En. Sec. 11, Ch. 632, L. 1987; amd. Sec. 4, Ch. 657, L. 1989.

Compiler'sComments

1989 Amendment Inserted (1)(j) regarding information request ed pursuant to subpoena; inserted (2) regarding disclosure prohibited by law; corrected internal reference; and mad$_{e}$ minor changes in phraseology and form.

Cross-References

Government health care information – legal proceedings, SO-16-605.

50-16-536. Method of compulsory process. (1) Unless the court for good cause shown determines that the notification should be waived or modified, if health care information is sought under 50-16-535 (l)(b), (l)(d), or (1)(e) or in a civil proceeding or investigation under 50-16-535 (l)(i), the person seeking discovery or compulsory process shall mail a notice by first-class mail to the patient or the patient's attorney of record of the compulsory process or discovery request at least 10 days before presenting the certificate required under subsection (2) to the health care provider,

(2) Service of compulsory process or discovery requests upon a health care provider must be accompanied by a written certification, signed by the person seeking to obtain health care information or his authorized representative, identifying at least one subsection of 50-16-535 under which compulsory process or discovery is being sought. The certification must also state, in the case of information sought under 50-16-535 (1)(b), (1)(d), or (1)(e) or in a civil proceeding under 50-16-535 (l)(i), that the requirements of subsection (1) for notice have been met. A person may sign the certification only if the person reasonably believes that the subsection of 50-16-535 identified in the certification provides an appropriate basis for the use of discovery or compulsory process. Unless otherwise ordered by the court, the health care provider shall maintain a copy of the process and the written certification as a permanent part of the patient's health care information.

(3) In response to service of compulsory process or discovery requests, where authorized by law, a health care provider may deny access to the requested health care information. Additionally, a health care provider may deny access to the requested health care information under 50-16-542(1). If access to requested health care information is denied by the health care provider under 50- 16-542(1), the health care provider shall submit to the court by affidavit or other reasonable means an explanation of why the health care provider believes the information should be protected from disclosure.

(4) Where access to health care is denied under 50-16-542(1), the court may order disclosure of health care information, with or without restrictions as to its use, as the court considers necessary, In deciding whether to order disclosure, the court shall consider the explanation submitted by the health care provider, the reasons for denying access to health care information set forth in 50- 16-542(1), and any arguments presented by interested parties.

(5) A health care provider required to disclose health care information pursuant to compulsory process may charge a reasonable fee, not to exceed

the health care provider's actual cost for providing the information, and may deny examination or copying of the information until the fee is paid.

(6) Production of health care information under 50-16-535 and this section does not in itself constitute a waiver of any privilege, objection, or defense existing under other law or rule of evidence or procedure.

History **En. Sec. 12, Ch. 632, 1.. 1987; amd. Sec. 5, Ch. 657, I.. 1989.**

Compiler's Comments

1989 Amendment: Inserted (3) regarding denial of access to information in response to compulsory process or discovery requests; inserted (4) relating to court-ordered disclosure; inserted (5) allowing a fee for providing information; and corrected internal references.

50-16-537 through 50-16-540 reserved.

50-16-541. **Requirements and procedures for patient's examination and copying.** (1) Upon receipt of a written request from a patient to examine or copy all or part of his recorded health care information, a health care provider, as promptly as required under the circumstances but no later than 10 days after receiving the request, shall:

(a) make the information available to the patient for examination during regular business hours or provide a copy, if requested, to the patient;

(b) inform the patient if the information does not exist or cannot be found;

(c) if the health care provider does not maintain a record of the information, inform the patient and provide the name and address, if known, of the health care provider who maintains the record;

(d) if the information is in use or unusual circumstances have delayed handling the request, inform the patient and specify in writing the reasons for the delay and the earliest date, not later than 21 days after receiving the request, when the information will be available for examination or copying or when the request will be otherwise disposed of; or

(e) deny the request in whole or in part under 50-16-542 and inform the patient.

(2) Upon request, the health care provider shall provide an explanation of any code or abbreviation used in the health care information. If a record of the particular health care information requested is not maintained by the health care provider in the requested form, he is not required to create a new record or reformulate an existing record to make the information available in the requested form. The health care provider may charge a reasonable fee, not to exceed the health care provider's actual cost, for providing the health care information and is not required to permit examination or copying until the fee is paid.

History En, ('h. 632, L. 1987.

50-16-542. Denial of examination and copying. (1) A health care provider may deny access to health care information by a patient if the health care provider reasonably concludes that:

(a) knowledge of the health care information would be injurious to the health of the patient;

(b) knowledge of the health care information could reasonably be expected to lead to the patient's identification of an individual who provided the information in confidience and under circumstances in which confidentiality was appropriate e;

(c) knowledge of the health care information could reasonably be expected to cause danger to the life or safety of any individual;

(d) the health care information was compiled and is used solely for litigation, quality assurance, peer review, or administrative purposes;

(e) the health care information might disclose birth out of wedlock orprovide information from which knowledge of birth out of wedlock might be obtained and which information is protected from disclosure pursuant to 50-15-206;

(f) the health care provider obtained the in formation from a person other than the patient; or

(g) access to the health care information is other wise prohibited by law.

(2) Except as provided in 50-16-521, a health care provider may deny access to health care information by a patient who is a minor if:

(a) the patient is committed to amental health facility; or

(b) the patient's parents or guardian have not authorized the health care provider to disclose the patient's health care information.

(3) If ahealth care provider denies are quest for examination and copying under this section, the provider, to the extent possible, shall segregate health care information for which access has been denied under subsection (1) from information for which access cannot be denied and permit the patient to examine or copy the disclosable information.

(4) If a health care provider denies a patient's request for examination and copying, in whole or in part, under subsection (l)(a) or (l)(c), he shall permit examination and copying of the record by another health care provider who is providing health care services to the patient for the same condition as the health care provider denying the request, The health care provider denying the request shall inform the patient of the patient's right to select another health care provider under this subsection.

History: En, Sec. 14, Ch. 632, L. 1987; amd. Sec. 6, Ch. 657, L. 1989.

Compiler's Comments

1989 *Amendment.* Inserted (1)(e) regarding information that might reveal birth out of wedlock.

50-16-543. Request for correction or amendment. (1) For purposes of accuracy or completeness, a patient may request in writing that a health care provider correct or amend its record of the patient's health care information to which he has access under 50-16-541.

(2) As promptly as required under the circumstances but no later than 10 days after receiving a request from a patient to correct or amend its record of the patient's health care information, the health care provider shall:

(a) make the requested correction or amendment and inform the patient of the action and of the patient's right to have the correction or amendment sent to previous recipients of the health care information in question;

(b) inform the patient if the record no longer exists or cannot be found;

(c) if the health care provider does not maintain the record, inform the patient and provide him with the name and address, if known, of the person who maintains the record;

(d) if the record is in use or unusual circumstances have delayed the handling of the correction or amendment request, inform the patient and specify

in writing the earliest date, not later than 21 days after receiving the request, when the correction or amendment will be made or when the request will otherwise be disposed of; or

(e) 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.

History: En. ***Sec. 15,*** Ch. 632. 1,. 1987.

50-16-544. Procedure for adding correction, amendment, or statement of disagreement. (1) In making a correction or amendment, the health care provider shall:

(a) add the amending information as a part of the health record; and

(b) mark the challenged entries as corrected or amended entries and indicate the place in the record where the corrected or amended information is located, in a manner practicable under the circumstances.

(2) If the health care provider maintaining the record of the patient's health care information refuses to make the patient's proposed correction or amendment, the provider shall:

(a) permit the patient to file as a part of the record of his health care information a concise statement of the correction or amendment requested and the reasons there for; and

(b) mark the challenged entry to indicate that the patient claims the entry is inaccurate or incomplete and indicate the place in the record where the statement of disagreement is located, in a manner practicable under the circumstances.

History: En. Sec. 16, (C h. 632, 1..1987.

50-16-545, Dissemination of corrected or amended information or statement of disagreement. (1) A health care provider, upon request of a patient, shall take reasonable steps to provide copies of corrected or amended information or of a statement of disagreement to all persons designated by the patient and identified in the health care information as having examined or received copies of the information sought to be corrected or amended.

(2) A health care provider may charge the patient a reasonable fee, not exceeding the provider's actual cost, for distributing corrected or amended information or the statement of disagreement, unless the provider's error necessitated the correction or amendment.

H istor~: En. Sec. 17, Ch. 632, 1,. 1987.

50-16-546 through 50-16-550 reserved.

50-16-551. Criminal penalty. (1) A person who by means of bribery, theft, or misrepresentation of identity, purpose of use, or entitlement to the information examines or obtains, in Violation of this part, health care information maintained by a health care provider is guilty. of a misdemeanor and upon conviction is punishable by a fine not exceeding $10,000 or imprisonment for a period not exceeding 1 year, or both.

(2) A person who, knowing that a certificate ion under 50-16-536(2) or a disclosure authorization under 50-16-526 and 50-16-527 is false, purposely

presents the certification or disclosure authorization to a health care provider is guilty of a misdemeanor and upon conviction is punishable by a fine not exceeding $10,000 or imprisonment for a period not exceeding 1 year! or both.

History: **En. Sec. 23, (Ch. 632, L. 1987.**

Cross-References

Government health care information -- penalty, 50-16-611.

Unauthorized divulgence of serological test information, 50-19-108.

50-16-552. Civil enforcement. The. attorney general or appropriate county attorney may maintain a civil action to enforce this part. The court may order any relief authorized by 50-16-553.

History **En. Sec. 14, ('h.** 632, **L,.** 1987.

50-16-553. Civil remedies. (1) A person aggrieved by a violation of this part may maintain an action for relief as provided in this section.

(2) The court may order the health care provider or other person to comply with this part and may order any other appropriate relief.

(3) A health care provider who relies in good faith upon a certification pursuant to 50-16-536(2) is not liable for disclosures made in reliance on that certification.

(4) No disciplinary or punitive action may be taken against a health care provider or his employee or agent who brings evidence of a violation of this part to the attention of the patient or an appropriate authority}'.

(5) In an action by a patient alleging that health care information was improperly withheld under 50-16-541 and 50-16-542, the burden of proof is on the health care provider to establish that the information was properly withheld.

(6) If the court determines that there is a violation of this part, the aggrieved person is entitled to recover damages for pecuniary losses sustained as a result of the violation and, in addition, if the violation results from willful or grossly negligent conduct, the aggrieved person may recover not in excess of $5,000, exclusive of any pecuniary loss.

(7) If a plaintiff prevails, the court may assess reasonable attorney fees and all other expenses reasonably' incurred in the litigation.

(8) An action under this part is barred unless the action is commenced within 3 years after the cause of action accrues.

History: En.Sec. **25,** Ch. **632,** L. **1987.**

AMER1CAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

HEALTH INFORMATION MODEL LEGISLATION LANGUAGE

SEC. 101. PREAMBLE

The Congress finds that: --

(a) The right of privacy is a personal and fundamental right protected by the Constitution of the United States;

(b) Health care information is personal and sensitive information that, if improperly used or released, may do significant harm to a patient's interests in privacy and in health care, and may affect a patient's ability to obtain employment, education, insurance, credit, and other necessities;

(c) patients need access to their own health care information as a matter of fairness to enable them to make informed decisions about their health care and correct inaccurate or incomplete information about themselves;

(d) Persons maintaining health care information need clear and certain rules for the disclosure of health care information;

(e) Persons other than health care providers obtain, use, and disclose health care information in many different contexts and for many different purposes. A patient's interest in the proper use and disclosure of the personal health care information continues even when the information has been initially Disclosed and is held by persons other than health care providers; and

(f) The movement of patients and their health care information across state lines, access to and exchange of health care information from automated data banks and networks, and the emergence of multi-state health care providers and payers creates a compelling need for Federal law, rules and procedures governing the use and disclosure of health care information.

SEC. 102. GENERAL DEFINITIONS.

In this [Act] (except as otherwise provided):

(a) AUDIT. --The term "audit" means an assessment, evaluation, determination, or investigation of a person maintaining health care information or health care rendered by such a

person by a person not employed by or affiliated with the person audited to determine compliance with--

(1) statutory, regulatory, fiscal, administrative. medical, or scientific standards;

(2) the requirements of a private or public program of payment for health care; or

(3) requirements for licensure, accreditation, or certification.

(b) COMPULSORY DISCLOSURE. --The term "compulsory disclosure" means any disclosure of health care information mandated or required by Federal or State law in connection with a judicial, legislative, or ach-ministrative proceeding, including but not limited to, disclosure required by subpoena, subpoena duces tecum, request Or notice to produce, court order, or any other method of requiring a person maintaining health care information to produce health care information under the criminal or civil discovery laws of any State or Federal government or administrative agency thereof.

(c) HEALTH CARE. --The term "health care" means:–

(1) any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure provided by a health care provider: --

(A) with respect to a patient's physical or mental condition; or

(B) affecting the structure or fiction of the human body or any part thereof, including, but not limited to, banking of blood, sperm, organs, or any other tissue; and

(2) any sale or dispensing of any drug, substance, device, equipment, or other iter to a patient or for a patient's use, pursuant to a prescription.

(d) HEALTH CARE INFORMATION. --The term "health care information" means 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.

(e) HEALTH CARE PROVIDER. --The term "health care provider" means a person w-ho is licensed, certified, registered or otherwise authorized by law to provide health care in the ordinary course of business or practice of a profession.

(f) INSTITUTIONAL REVIEW BOARD. --The term "institutional review board" means any board, committee, or other group formally designated by an institution, or authorized under Federal or State law, to review, approve the initiation of, or conduct periodic review of, research programs to assure the protection of the rights and Welfare of human research subjects.

(g) MAINTAIN.--The term "maintain," as related to health care information, means to create, collect, handle, hold, possess, preserve, retain, store, control or transmit such information.

(h) PATIENT. --The term "patient" means an individual who receives or has received health care. The term includes a deceased individual who has received health care.

(i) PATIENT'S AUTHORIZATION. --The term "patient's authorization" means an authorization that is valid under the provisions of Section 104.

('j) PATIENT REPRESENTATIVE. --The term "patient representative" shall mean am individual legally empowered to make decisions concerning a patient's health care or the administrator or executor of a deceased patient's estate.

(k) PERSON. --The term "person" means--

(1) an individual, corporation, business trust, estat, trust, partnership, association, joint venture, or any other legal or commercial entity: and

(2) except for purposes of Section 111 and 112. a government, governmental subdivision, agency or authority.

(1) SECRETARY. --The term "Secretary" means the Secretary of Health and Human Services.

SEC. 103. DISCLOSURE.

(a) DISCLOSURE.--NO person other than a patient or patient representative may disclose health care information to any other person without the patient's authorization, except as authorized in Section 105. No person may disclose health care information under a patient's authorization, except in accordance with the terms of such authorization. The provisions of this paragraph shall apply both to disclosures of health care information and to redisclosures of health care information by a person to whom health care information is disclosed.

(b) RECORD OF DISCLOSURE. --Each person maintaining health care information shall maintain a record of all external disclosures of health care information made by such person concerning each patient, and such record shall become part of the health care information concerning each patient. The record of each disclosure shall include the name, address and institutional affiliation, if any, of the person to whom the health care information is disclosed, the date and purpose of the disclosure and, to the extent practicable, a description of the information disclosed.

SEC. 104. PATIENT'S AUTHORIZATION; REQUIREMENTS FOR VALIDITY.

(a) To be valid, a patient's authorization must--

(1) Identify the patient;

(2) Generally describe the health care information to be disclosed;

(3) Identify the person to whom the health care information is to be disclosed;

(4) Describe the purpose of the disclosure;

(5) Limit the length of time the patient's authorization will remain valid;

(6) Be given by one of the following means--

(A) In writing, dated and signed by the patient or the patient representative; or

(B) In electronic form, dated and authenticated by the patient or the patient representative using a unique identifier; and

(7) Not have been revoked under paragraph (b).

(b) REVOCATION OF PATIENT'S AUTHORIZATION. --A patient or patient representative may revoke the patient's authorization at any time, unless disclosure is required to effectuate payment for health care that has been provided to the patient, or other substantial action has been taken in reliance on the patient's authorization. A patient may not maintain an action against a person for disclosure of health care information made in good faith reliance on the patient's authorization, if the person had no notice of the revocation of the patient's authorization at the time disclosure was made.

(c) RECORD OF PATIENT'S AUTHORIZATIONS AND REVOCATIONS .--Each person maintaining health care information shall maintain a record of all patient's authorizations and revocations thereof, and such record shall become part of the health care information concerning each patient.

(d) NO WAIVER. --Except as provided by this [Act], the signing or authentication of an authorization by a patient or patient representative is not a waiver of any rights a patient has under other Federal or State statutes, the rules of evidence, or common law.

SEC. 105. DISCLOSURE WITHOUT PATIENT'S AUTHORIZATION.

A person maintaining health care information may disclose health care information about a patient without the patient's authorization as follows: --

(a) DISCLOSURE TO THE PATIENT OR PATIENT REPRESENTATIVE. --Any disclosure of patient information to the patient or such patient's patient representative;

(b) DISCLOSURE BY FAMILY AND FRIENDS. --Any disclosure of health care information by a family member or by any other individual with whom the patient has a personal relationship, provided that: --

(1) the health care information was disclosed to such individual by the patient or otherwise not in violation of this [Act]; and

(2) the health care information was not disclosed to the individual making the disclosure in the course of providing health care to the patient;

(c) DISCLOSURE TO EMPLOYEES AND AGENTS .--Disclosure, to the extent necessary for the disclosing person to carry out its lawful activities, to the disclosing person's agent, employee, or independent contractor who is under a legal obligation to hold the health care information in confidence and not to use such health care information for any purpose other than the lawful purpose for which the health care information was obtained by the disclosing person;

(d) DISCLOSURE TO ANOTHER HEALTH CARE PROVIDER. --Disclosure to a health care provider who is providing health care to the patient except as such disclosure is limited or prohibited by the patient;

(e) DISCLOSURE TO AVOID DANGER. --Disclosure to any person to the extent the recipient needs to know the information, if the person holding the health care information reasonably believes that such disclosure will avoid or minimize imminent danger to the health or

safety of the patient or any other individual, or is necessary to alleviate emergency circumstances affecting the health or safety of any individual;

(f) DISCLOSURE TO FAMILY. --Disclosure to a member of the patient's immediate family, or to any other individual with whom the patient is known to have a close personal relationship, if such disclosure is made in accordance with good medical or other professional practice, except as such disclosure is limited or prohibited by the patient;

(g) DISCLOSURE TO SUCCESSOR IN INTEREST. -Disclosure to a person who is a successor in interest to the person maintaining the health care information, provided, howe~'er, that no person other than a licensed health care provider or the spouse of a deceased health care provider shall be considered a successor in interest to a health care provider;

(h) DISCLOSURE TO GOVERNMENTAL AUTHORITIES .--Disclosure to Federal, State, or local governmental, authorities, to the extent the perwn holding the health care information is required by law to report specific health care information: --

(1) when needed to determine compliance with State or Federal licensure, certification, or registration rules or laws; or

(2) when needed to protect the public health;

(i) DISCLOSURE FOR AUDITS. --Disclosure to a person who obtains health care information solely for purposes of an audit, if that person agrees in writing: --

(1) to remove from the health care information or destroy, at the earliest opportunity consistent with the purpose of the audit, information that would enable identification of the patient;

(2) not to disclose in any public report any medical information; and

(3) not to further disclose the health care information, except to accomplish the audit or to report unlawful or improper conduct involving health care payment fraud by a health care provider or a patient, or other unlawful conduct by the health care provider;

(j) DISCLOSURE FOR RESEARCH. --Disclosure for use in a research project:

(1) that an institutional review board has determined: --

(A) is of sufficient importance to outweigh the intrusion into the privacy of the patient that would result from the disclosure;

(B) is reasonably impracticable without the use or disclosure of the health care information in individually identifiable form;

(C) contains reasonable safeguards to protect the information from redisclosure;

(D) contains reasonable safeguards to protect against identifying, directly or indirectly, any patient in any report of the research project; and

(E) contains procedures to remove or destroy at the earliest opportunity, consistent with the purposes of the project, information that would enable identification of the patient, unless the institutional review board authorizes retention of identifying information for purposes of another research project; and

(2) if the person agrees in writing: --

(A) to remove from the health care information or destroy, at the earliest opportunity consistent with the purpose of the research project, information that would enable identification of the patient;

(B) not to disclose health care information in any public report; and

(C) not to further disclose the health care information, except as necessary to conduct the research project approved by the institutional review board.

(k) COMPULSORY DISCLOSURE. --Compulsory disclosure in accordance with the requirements of Section 108;

(1) DISCLOSURE TO LAW ENFORCEMENT AUTHORITIES .--Disclosure to Federal, State or local law enforcement authorities to the extent required by law;

(m) DISCLOSURE DIRECTED BY A COURT. --Disclosure directed by a court in connection with a court-ordered examination of a patient; or

(n) DISCLOSURE TO IDENTIFY A DECEASED INDIVIDUAL. --Disclosure based on reasonable grounds to believe that the information is needed to assist in the identification of a deceased individual.

SEC. 106. STANDARDS FOR INFORMATION PRACTICES.

(a) PROMULGATION OF REQUIREMENTS---

(1) IN GENERAL. --Between July 1, 1994, and July 1, 1995, the Secretary shall promulgate requirements for information practices of persons maintaining health care information. Such requirements shall be consistent with the provisions of this [Act] and shall be in accordance with the principles set forth in paragraph (b).

(2) REVISION. --The Secretary may from time to time revise the requirements promulgated under this paragraph.

(b) PRINCIPLES OF FAIR INFORMATION PRACTICES. --The requirements promulgated under paragraph (a) shall incorporate the following principles:

(1) PATIENT'S RIGHT TO KNOW. --The patient or the patient representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purposes the health care information is used;

(2) RESTRICTIONS ON COLLECTION. --Health care information concerning a patient must be collected only the extent necessary to carry out the legitimate purpose for which the information is collected;

(3) COLLECTION AND USE ONLY FOR LAWFUL PURPOSE. --Health care information must be collected and used only for a necessary and lawful purpose;

(4) NOTIFICATION TO PATIENT. Each person maintaining health care information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy of the statement of the person's fair information practices and should receive an explanation of such fair information practices upon request;

(5) RESTRICTION ON USE FOR OTHER PURPOSES. --Health care information may not be used for any puposes beyond the purposes for which the health care information collected, except as otherwise provided in this [Act];

(6) RIGHT TO ACCESS .--The patient or the patient representative may have access to health care information concerning the patient has the right to have a copy of such health care information made after payment of a reasonable charge, and, futher, has the right to have a notation made with or in such health care information of any amendment

or correction of such health care information requested by the patient or patient representative;

(7) REQUIRED SAFEGUARDS.--Any person maintaining, using or disseminating health care information shall implement reasonable safeguards for the security of the health care information and its storage, processing and transmission, whether in electronic or other form;

(8) ADDITIONAL PROTECTIONS. --Methods to ensure the accuracy, reliability, relevance, completeness and timeliness of health care information should be instituted; and

(9) ADDITIONAL PROTECTIONS FOR CERTAIN HEALTH CARE INFORMATION .--If advisable, provide additional safeguards for highly sensitive health care information (such as health care information concerning mental health, substance abuse, communicable and genetic diseases, and abortions. as well as health care information concerning celebrities and notorious individuals, and health care information contained in adoption records).

SEC. 107. OBLIGATIONS OF PATIENT REPRESENTATIITS.

(a) AUTHORITY OF PATIENT REPRESENTATIVES .--A person authorized to act as a patient representative may exercise the rights of the patient under this [Act] to the extent necessary to effectuate the terms or purposes of the grant of authority; but a patient who is a minor and who is authorized to consent to health care without tie consent of a parent or legal guardian under State law may exclusively exercise the rights of a patient under this [Act] as to information pertaining to health care to which the minor lawfully consented.

(b) GOOD FAITH OBLIGATION.--A patient representative shall act in good faith to represent the best interests of the patient with respect to health care information concerning the patient.

SEC. 108. COMPULSORY DISCLOSURE.

(a) LIMITS ON COMPULSORY DISCLOSURE.--NO person may be compelled to disclose health care information maintained by such person pursuant to a request for compulsory disclosure in any judicial, legislative or administrative proceeding, unless:

(1) The person maintaining the health care information has received a patient's authorization to release the health care information in response to such request for compulsory disclosure;

(2) The patient has knowingly and voluntarily waived the right to claim privilege or confidentiality for the health care information sought;

(3) The patient is a party to the proceeding and has placed his or her physical or mental condition in issue;

(4) The patient's physical or mental condition is relevant to the execution or witnessing of a will;

(5) The physical or mental condition of a deceased patient is placed in issue by any person claiming or defending through or as a beneficiary of the patient;

(6)Health care information concerning the patient is to be used in the patient's commitment proceeding;

(7) The health care information is for use in any- law enforcement proceeding or investigation in which a health care provider is the subject or a party; provided, however, that health care information so disclosed shall not be used against the patient, unless the matter relates to payment for the patient's health care, or unless compulsory disclosure is ordered as authorized under subparagraph (9);

(8) The health care information is relevant to a proceeding brought under Section 110, 111, or 1 12; or

(9) The court or Federal or State agency or Congress or the State legislature has determined, after hearing any objections made pursuant to paragraph (d), that particular health care information is subject to compulsory disclosure because the party seeking the health care information has demonstrated that the interest that would be served by disclosure outweighs the patient's privacy interest,

(b) NOTICE REQUIREMENT. Unless the court, or Federal or State agency or Congress or State legislature, for good cause shown, determines that the notification should be waived or modified, if health care information is sought under subparagraph (2), (4) or (5), or in a civil proceeding or investigation pursuant to subparagraph (9), the person requesting compulsory disclosure shall serve upon the person maintaining the health care information and upon the patient, the patient's legal guardian or other person legally authorized to act for the patient in such a matter, or on the patient's attorney, the original or a copy of the compulsory disclosure request at least thirty (30) days in advance of the date on which compulsory disclosure is requested and a statement of the right of the patient and of the person maintaining the health care information to have any objections to such compulsory disclosure heard by such court, or governmental agency or Congress or State legislature prior to the issuance of an order for such

compulsory disclosure and the procedure to be followed to have any such objection heard. Such service shall be made by certified mail, return receipt requested, or by hand delivery, in addition to any form of service required by applicable State or Federal law. The notice requirements of this paragraph shall not apply to a request for compulsory disclosure of health care information relating to a patient if made by or on behalf of a patient.

(c) CERTIFICATION UNDER OATH.

(1) A person seeking compulsory disclosure of health care information about a patient under this section shall provide the person maintaining the health care information from whom compulsory disclosure is sought with a written certification under oath by the person seeking such compulsory disclosure or an authorized representative of such person :--

(A) identifying each subparagraph of paragraph (a) under which compulsory disclosure of health care information is being sought; and

(B) stating that notice has been provided in accordance with the requirements of paragraph (b) or is not required by paragraph (b) with respect to any of the health care information sought.

(2) A person may sign a certification described in subparagraph (l), only if the person reasonably believes that the subparagraph or subparagraphs of paragraph (a) identified in the certification provide an appropriate basis for the use of a request for compulsory disclosure.

(d) OBJECTION TO COMPULSORY DISCLOSURE .--If the person maintaining health care information or the patient or the patient's legal guardian or attorney or other person legally authorized to represent the patient in such a matter files in the manner set forth in the notice described in paragraph (b) such person's objection to the request for compulsory disclosure prior to the date on which such compulsory disclosure is sought, the burden shall be on the person requesting such compulsory disclosure to seek an order from the appropriate court or Federal or State agency or State legislature or Congress an order compelling such disclosure, and the person or persons filing such objection may defend in any proceeding to compel such disclosure.

(e) MAINTENANCE OF NOTICE AND CERTIFICATION. Unless otherwise ordered by the court, State or Federal agency, Congress or State legislature, a person maintaining health care information shall maintain a copy of each request for compulsory disclosure and accompanying certification as part of the patient's health care information.

(f) NO WAIVER. --Disclosure of health care information pursuant to compulsory disclosure, in and of itself, shall not constitute a waiver of any privilege, objection, or defense existing under any other law or rule of evidence or procedure.

SEC. 110. CIVIL REMEDIES.

(a) PRIVATE RIGHT OF ACTION. --A person aggrieved by a violation of this [Act] may maintain an action for relief as provided in this section.

(b) JURISDICTION. --The district courts of the United States shall have jurisdiction in any action brought under the provisions of this section.

(c) RELIEF. --The court may order a person maintaining health care information to comply with this [Act] and may order any other appropriate relief.

(d) DAMAGES.--If the court determines that there is a violation of this [Act], the aggrieved person is entitled to recover damages for any losses sustained as a result of the violation; and, in addition, if the violation results from willful or grossly negligent conduct, the aggrieved person may recover not in excess of [$ 10,000], exclusive of any loss.

(e) ATTORNEYS' FEES.--If a plaintiff prevails in an action brought under this section, the court, in addition to any other relief granted under this section, may award the plaintiff reasonable attorneys' fees and all other expenses incurred by the plaintiff in the litigation.

(f) STATUTE OF LIMITATIONS .--Any action under this [Act] must be brought within two years from the date the alleged violation is discovered.

SEC. 111. CIVIL MONEY PENALTIES.

(a) Any person that knowingly discloses or health care information in violation of this [Act] shall be subject, in addition to any other penalties that maybe prescribed by law--

(1) to a civil money penalty of not more than [$1 ,000] for each violation, but not to exceed [$25,000] in the aggregate for multiple violations, except as provided in subparagraph (2); and, in addition--

(2) to a civil money penalty of not more than [$1,000,000] if the Secretary finds that violations of this [Act] have occurred in such numbers or with such frequency as to constitute a general business practice.

SEC. 112. CRIMINAL PENALTY FOR OBTAINING HEALTH CARE INFORMATION THROUGH FALSE PRETENSES OR THEFT.

(a) Any person who, under false or fraudulent pretenses or with a false or fraudulent certification required under this [Act], requests or obtains health care information from a person maintaining health care information or a patient's authorization shall be fined not more than $10,000 or imprisoned not more than six months, or both, for each offense.

(b) Anv person who, under false or fraudulent pretenses or with a false or fraudulent certification required under this [Act], requests or obtains health care information from a person maintaining health care information and who intentionally uses, sells or transfers such health care information for remuneration, for profit or for monetary gain shall be fined not more than $50,000, or imprisoned for not more than two years, or both, for each offense.

(c) Any person who unlawfully takes health care information from a person maintaining health care information and who intentionally uses, sells or transfers such health care information for remuneration, for profit or for monetary gain shall be fined not more than $50,000, or imprisoned for not more than two years, or both, for each offense.

SEC. 113. PREEMPTION OF STATE LAWS.

(a) Effective as of the effective date of this [Act], no State may establish or enforce any law or regulation concerning the disclosure of health care information, except as provided in paragraph (b).

(b) This [Act] does not supersede any restriction on the disclosure or use of health care information under: --

(1) any Federal, or State law on the inspection of, or disclosure or use of health care information relating to alcohol or drug abuse, or health care for such abuse;

(2) any Federal,, or State law concerning the disclosure or use of health care information relating to psychiatric, psychological, mental health or developmental disabilities health care;

(3) Section 1106 of the Social Security Act;

(4) Section 1160 of the Social Security Act; or

(5) any Federal or State law making information. including but not limited to health care information, that is maintained, used or generated in the course of

peer review, quality assurance, or similar activities or functions privileged or confidential.

(c) Nothing in this [Act] shall be construed to make any Federal Government authority or any Federal agency subject to any State or local law not otherwise applicable.

SEC. 114. MISCELLANEOUS PROVISIONS.

(a) SEVERABILITY.--If any provision of this [Act] or its application to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of this [Act] that can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

Index

Abuse of medical information, 11-12,20,26-29, 75-76,81-82
Access issues
  access control technology, 54, 57-58, 62-63, %, 97-99
  increasing demands for computerized information, 6, 15-16,31,36,71
  management security controls, 90
  patient access to records, 17,70-73,76, 82-84
  secondary users of information, 16, 18, 20, 71,76, 84-85
  security breaches by ''insiders, ' 11-12, 90-91
Accreditation Manual for Hospitals, 63
Administration Task Force on Health Care Reform, 12
Administrative costs. See Cost savings
Alcohol and drug abuse laws, 14,42,72
AMA. See American Medical Association
American Health Information Management Association, 5, 17, 77, 80-82
American Hospital Association's Patient's Bill of Rights, 41
American Medical Association
  Council on Ethical and Judicial Affairs, 38,40-41
  ethics codes and principles, 14, 30, 38,43
  Model State legislation on Confidentiality of Health Care Information (American Medical Association), 4-5, 80
American National Standards Institute, 69
Audit trails, 54,96,97-99
Australia, smart card system proposal, 58,61

Back-up databases, 10, 13,63
Biometric authentication systems, **95-96**
Breach of contract, 43

Canada
  Commission d'Acces a I'Information, 85
  information brokering investigations, 28
  unique patient identifier use, 66
Card systems. See Smart cards
Cipher systems, 92-93
CLIPPER Chip, 93,94-95
Common law. See State laws and regulations
Communications linkage safeguards, %,98
Communications networks, 8-10,24,53
Computer architecture security measures, 96
The Computer-Based Patient Record, An Essential Technology for Health Care. See Institute of Medicine report
Computer-based Patient Record Institute, 24
Computer security. See ***also*** Implementing a computerized medical information system; Recordkeeping and information flow; Standards for computerized medical information; Technology of computerized medical information
  data and system security standards, 20-21,67
  data protection initiatives, 19,76-77
  management controls, 90-91
  online systems, 11-12, 54-55
  policy options, 20,76,85-86
  security policies, 35, 89-90

smart cards, 11-13, **55-64, 96**
technical safeguards, 86,91-99
technology and security, 6,9-10, 11-12, 36, 52
Computer service companies. See Private sector computerization of medical information
Computers and the Rights of Citizens, 77-78
Confidentiality of information. See *also* Computer security; Ethical origins of right to privacy; Ethical Tenets for Protection of Confidential Clinical Data; Right to privacy in medical information
alcohol and drug abuse laws, 14,42,72
defined, 4-5
privacy versus confidentiality, 6,7-9
standards for computerized medical information, 67
State law sources, 15,42-44
Consent. See Informed consent to disclosure of information
Constitution as source for right to privacy, 14,38, 39-40
Content standards. See Standards for computerized medical information
Cost savings, 9,23-24,53
Cryptography, 57-58,65,91-93,94-95

Data and system security standards. See Computer security; Standards for computerized medical information
Data comectivity, 8-10, 18, 24-25,52-53. See *also* Online systems
Data Encryption Standard, 58,93
Data-exchange standards. See Standards for computerized medical information
Data protection. See Computer security
Data Protection Board, 21
Defamation, 15,4243
Digital signatures, 91-92
Disclosure issues. See *aZso* Informed consent to disclosure of information; Privacy Act
effects of disclosure, 5-6, 29-30, 48, 50
Federal employees' disclosure, 11-12,26,29
State law sources of confidentiality obligation, 15, 42-44
Discnrninatory practices, 29-30
Doe v. Roe, **43**
Drug treatment. See Alcohol and drug abuse laws

Education of patients. See Patient education rules
Eisenstadt v. Baird, 39
Electronic Record Systems and Individual Priva(y, **79**
Encryption, 58,65,91. See *also* Cryptography
Encryption algorithms, 92-93
Ethical origins of right to privacy, 13-14, 15,30,38, 4041,43
Ethical Tenets for Protection of Confidential Clinical Data, 76-77, 80, 83, 84-85

Fair Credit Reporting Act, 33, 80
Fair information practices, 18-19,77-79
Family Educational Rights and Privacy Act, 80
Federal employees' disclosure of personal information, 11-12, 26, 29
Federal laws protecting privacy, 14-15, 19-20,41-42, 44,48-50,72, 79-80. See *also* Privacy Act
Federal Register, 78-79, 82
France, smart card system, 10,59-61

Greidinger v. Davis, 65
Griswold v. Connecticut, 14, 39

Hammonds v. Aetnu Casualty and Surety Co., 43
Health Cards and Numbers Control Act (Canada), 66
Health care cards, 58-64
Health care delivery-computerization relationship, 9, 23-24,37
Health Care Financing Administration, 31, 90
Health care industry records computerization, 6, 8-10
Health care information privacy committee, 87
Health care information protection schemes, 18-19,79
Health care reviews, 31,47
Health Insurance scheme (France), 59
Healthcare Informatics Standard Planning Panel, 69
High-performance computing networks, 53-54
Hospital recordkeeping, 4546,63

Identification cards, 10, 64
Identifiers for patients. See Unique patient identifiers
Implementing a computerized medical informaticm system. See *also* Computer security
informed consent to disclosure of information, 17, 20,69-74,76, 82
standardization of computerized medical information, 17-18, 20,53,66-69
technology of computerized medical information, 51-64

umque patient identifiers, 16-17, 64-66
Independent Commission Against Corruption of New South Wales, 28
Information brokering, 26, 28-29, 81
Information flow. See Recordkeeping and information flow
Information infrastructure, 8-10,53. See *also* Communications networks; Online systems
h]formation services. See Private sector computerization of medical information
Informed consent to disclosure of information, 17,20, 69-74, 76, 82
Institute of Medicine report
  computerization issues and concerns, 2, 6, 23-24
  data connectivity, 8-9, 12, 16, 52-53
  increasing demand for access to data, 18, 31
Insurance industry computerization of information, 11, 32-35
Insurance Information and Privacy Protection Model Act, 33
International data protection boards, 85, 87
International projects using smart cards, 59-62
IOM report, See Institute of Medicine report

Joint Commission on Accreditation of Healthcare Organizations, 31, 63

Kutz ~', United States, 39
Krever Commission ('Canada), 28

Legal origins of right to privacy, 14-15,41-44
Longitudinal patient records, 9, 24, 68-69

IManagement controls, 90-91
Marketing of medical information. See Abuse of medical infomlation; Private sector computerization of medical information
Massachusetts Institute of Technology, 93
Massachusetts law on Insurance Information and Privacy Protection, 76, 81, 82-83
Medical Information Bureau, 30, 32-33
Medical information definition, 2-5,20,68,75, 80-81
Medical Practices Acts, 43
Medicare peer review organization program, 31
Message authentication, 91
Model legislation language, ***5, 80-82***
Model State Legislation on Confidentiality of Health Care Information (American Medical Association), 4-5, 80
Models for protection of information, 18-19,75-77
Montana, Uniform Health Care Information Act, 77, 81

National Association of Insurance Commissioners, 33, 76
National Bureau of Standards, **93**
National identification card system, 10, 64
National Institute of Standards and Technology, **92,94**
National Practitioner Data Bank, 86
National Security Agency, **93,94**
New South Wales, Independent Commission Against Corruption of New South Wales, 28

Offline technology. See Smart cards
Online systems, 10, 11-12,26,52-55
Ownership of medical records, 70, 83

Passwords, 54, 94-95
Patient cards, 58-64
Patient concerns
  access to records, 17, 70-73, 76, 82-84
  disclosure to physician, 5-6, 30,48, 50
Patient education rules, 20,75-77, 82-84
Patient identifiers. See Unique patient identifiers
Patient records. See Longitudinal patient records; Medical information deftition; Patient concerns; Policy issues and options; Recordkeeping and information flow; Secondary users of medical data; Workgroup on Computerization of Patient Records report
Paul v. Davis, 40
PCS Health Systems, Inc., 34-35
Personal identification security techniques, **93-96**
Physician Computer Network, Inc., 33-34
Physicians. See *also* Ethical origins of right to privacy; Ethical Tenets for Protection of Confidential Clinical Data; Patient concerns
  recordkeeping by, 45, 48, 50, 63
  withholding of information by, 17, 71-72
Policy issues and options
  background and study approach, 1-5
  computerization of medical records, 6, 8-12
  computerization-related policy problems, 16-18

congressional options, 19-21, 75-76, 79-87
fair information practices and the Privacy AcC 18-19,77-79
models forprotection of information, 18-19,75-77
need for privacy in medical information, 5-6
privacy confidentiality,6, 7-9
protection of privacy in medical information, 12-16
technology proposals and challenges to privacy, 12-13
Port protection devices, 96,98
Primary uses of medical information, 2-3
Privacy Act
Federal agency requirements, 4142, 82
information brokering guidelines, 81
patient access to information, 72
provisions of, 18,74,77-79
and Social Security number as identifier, 65
Privacy definition, 6,7-9. See *also* Right to privacy in medical information
Privacy of Medical Information Bill of 1980, 81
Privacy oversight
Data Protection Board, 21
Health care information privacy committee, 87
Privacy Protection Study Commission, 72
Private sector computerization of medical information, 11, 30-31,32-35
Professional ethical codes. See Ethical origins of right to privacy; Ethical Tenets for Protection of Confidential Clinical Data
Public sector abuse of medical information, 11-12,26, 29
Public's concerns about privacy, 25-26

Reasonable use of medical information, 73-74
Recordkeeping and information flow
Federal legislation need, 44-50
standards for computerized medical information, 66-69
tracing information flow, 20, 76, 85-86
Right to Financial Privacy Act, 80
Right to privacy in medical information. See *also* Constitution as source for right to privacy; Ethical origins of right to privacy; I.egal origins of right to privacy; Policy issues and options; Privacy Act
computerization and privacy, 6, 8-12, 15-16,23-29, 36-37
defining violations and providing sanctions, 20, 75-76,81-82
importance of privacy, 5-6, 26, 28-30
and increased demands for information, 15-16, 18, 31,36,71
private sector computerization, 11, 30-31, 32-35
recordkeeping and information flow, 20, 44-50, 66-69,76,85-86
Social Security number as identifier, 16-17,65
Roe v. Wade, 40
RSA encryption system, 93

Sale of personal information. See Abuse of medical information; Private sector computerization of medical information
Secondary users of medical data
access protocols, 20, 76, 84-85
private sector computerization, 11, 30-31, 32-35
recordkeeping and information flow, 47-48
rising demand for records, 15-16, 18, 71
uses of patient records, 2-4, 5, 9
Secrecy definition, 7,9
Security modems, 95-96
Security of patient information. See Computer security
Security policies, 89-90
Smart cards
as access control means, 11, 12-13, 57-58
description, 10
French system, 10,59-61
as information storage means, 55-57
as medical data carrier, 58-64
personal identification techniques, 96
Social Security Act of New South Wales, 28
Social Security Act (United States), 14-15,65
Social Security Administration (United States), 29
Social Security number as identifier, 16-17,64-66
Social Security system (France), 59
Standards for computerized medical information, 17-18,20-21,53,66-69
State laws and regulations
congressional options, 19-21
Massachusetts law on Insurance Information and Privacy Protection, 76, 81, 82-83
patient access to health records, 72
sources of confidentiality obligation, 15, 4244
Uniform Health Care Information Act, 77,81,83-84
Storage of information on smart cards, 55-57
Supreme Court, 14,39-40

Technology of computerized medical information
computer security topics, 6, 10-13,20-21,86, 89-99
elements of computerized systems, 51-52
online systems, 52-55
smart cards, 52, 55-64
standards for information, 17-18, 20-21, 53, 66-69
Third-party payers, 31, 34-35,47
Token-based authentication systems, 95

Uniform Health Care Information Act, 77, 81, 83-84
Unique patient identifiers, 16-17,64-66
United States of America v. Westinghouse Electric, 6
United States v. Miller, 40
U.S. Department of Health, Education and Welfare, 77-78
U.S. Department of Health and Human Semices, 14-15
U.S. Social Security Administration, 29
User identification names. 54
User-specific menus, 54
User verification systems, 93-96

Videotape Privacy Protection Act, 80
Vocabulary standards. See Standards for computerized medical information

Washington, Uniform Health Care Information Act, 77, 81
WEDI report, See Work Group for Electronic Data Interchange report
Work Group for Electronic Data Interchange report
clarity problems with existing law, 44, 50
computerization issues and concerns, 9, 12, 24, 25
confidentiality of health information, 44
security technology, 90
Workgroup on Computerization of Patient Records report, 12, 25, 36

U.S. GOVERNMENT PRINTING OFFICE