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.

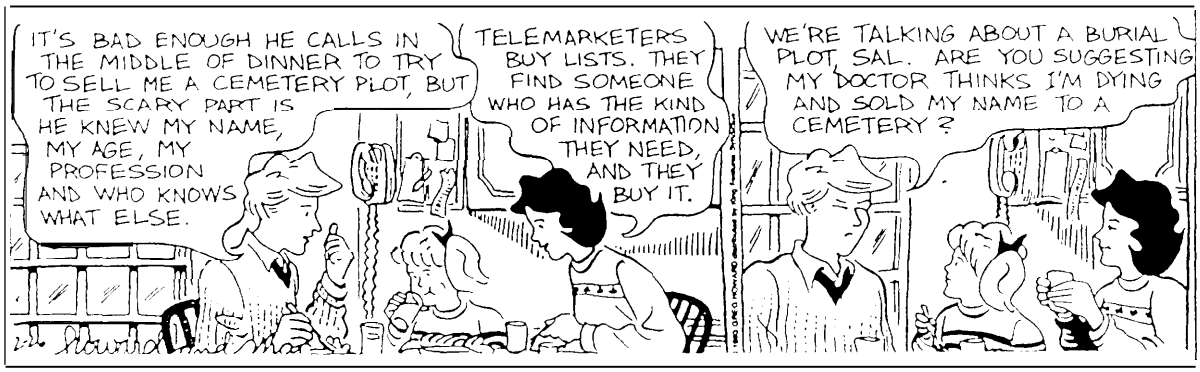
15 For example, is information on chronic health conditions, when used to determine whether or not to employ specific individuals, sensitive? Different persons will also vary in their perceptions of what is sensitive, and thus what constitutes an invasion of privacy may vary from person to person. Joan 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).

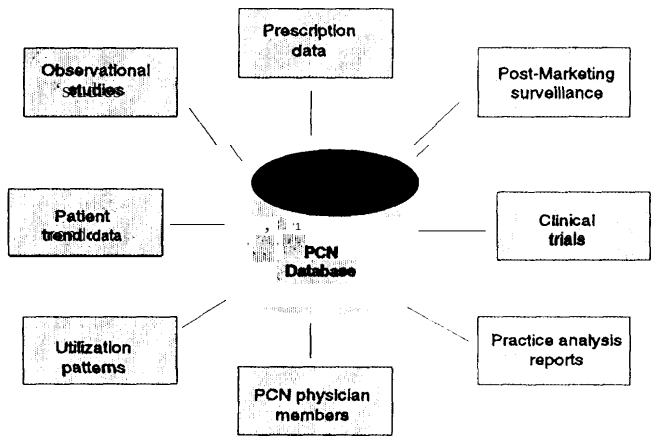
5 Michael Day, President, MIB, Inc., personal communication, April 1993.

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.

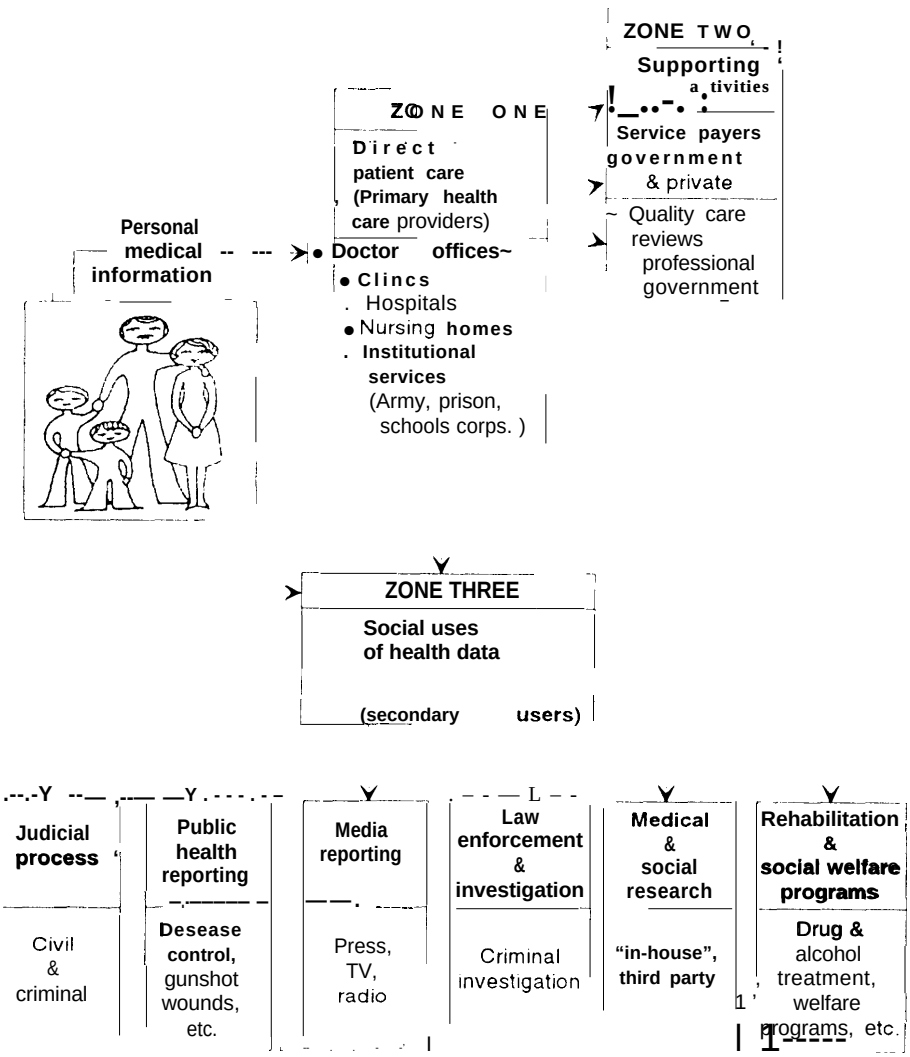
(continued on next page)

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.

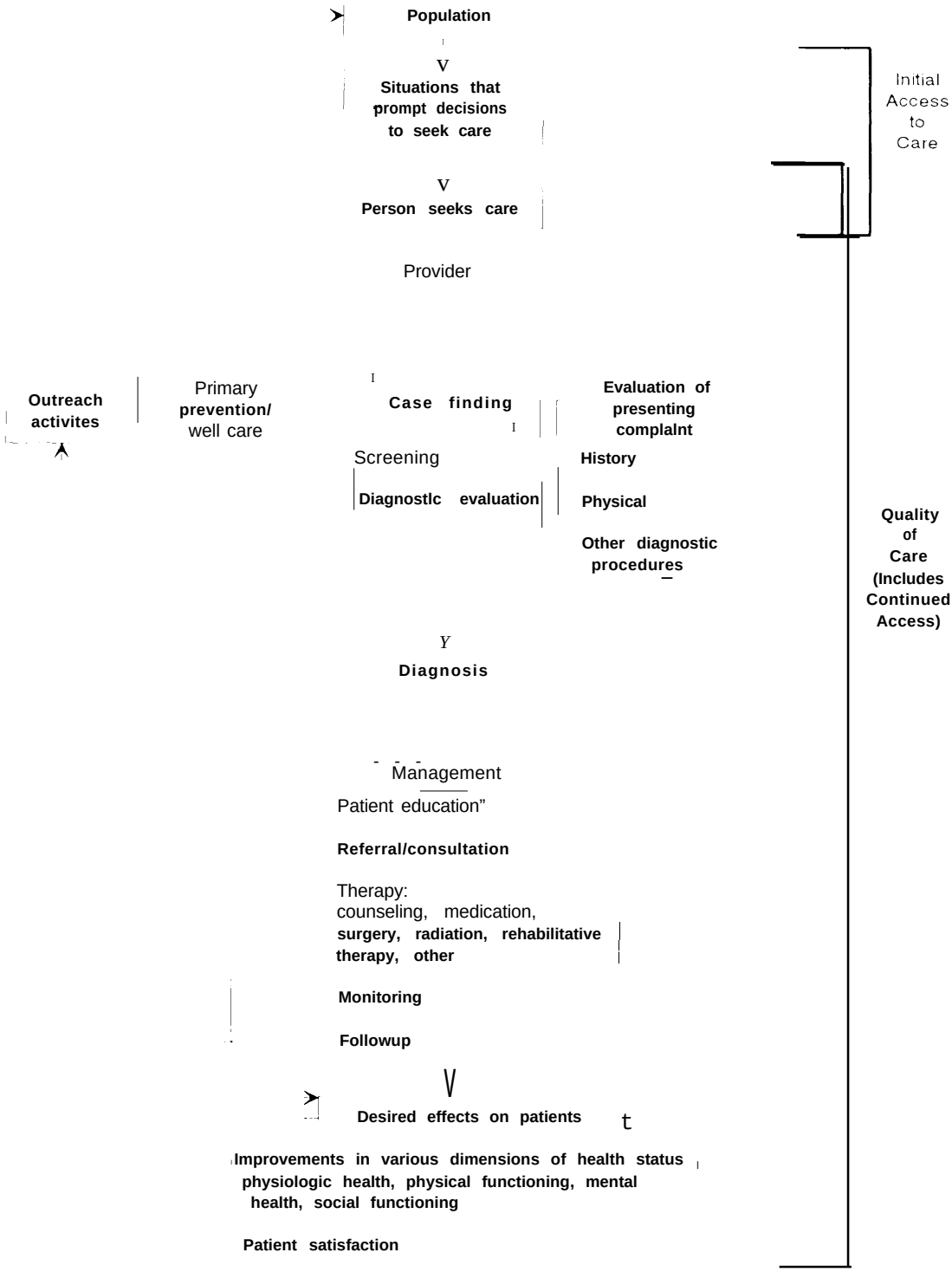
Patient awareness that records are maintained on computers, absent the assurance of a clear law protecting the confidentiality of those records, could lead to deterioration of the traditionally cofidential ''physician-patient' relationship.[57] Some contend that this breakdown could well lead to patients'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