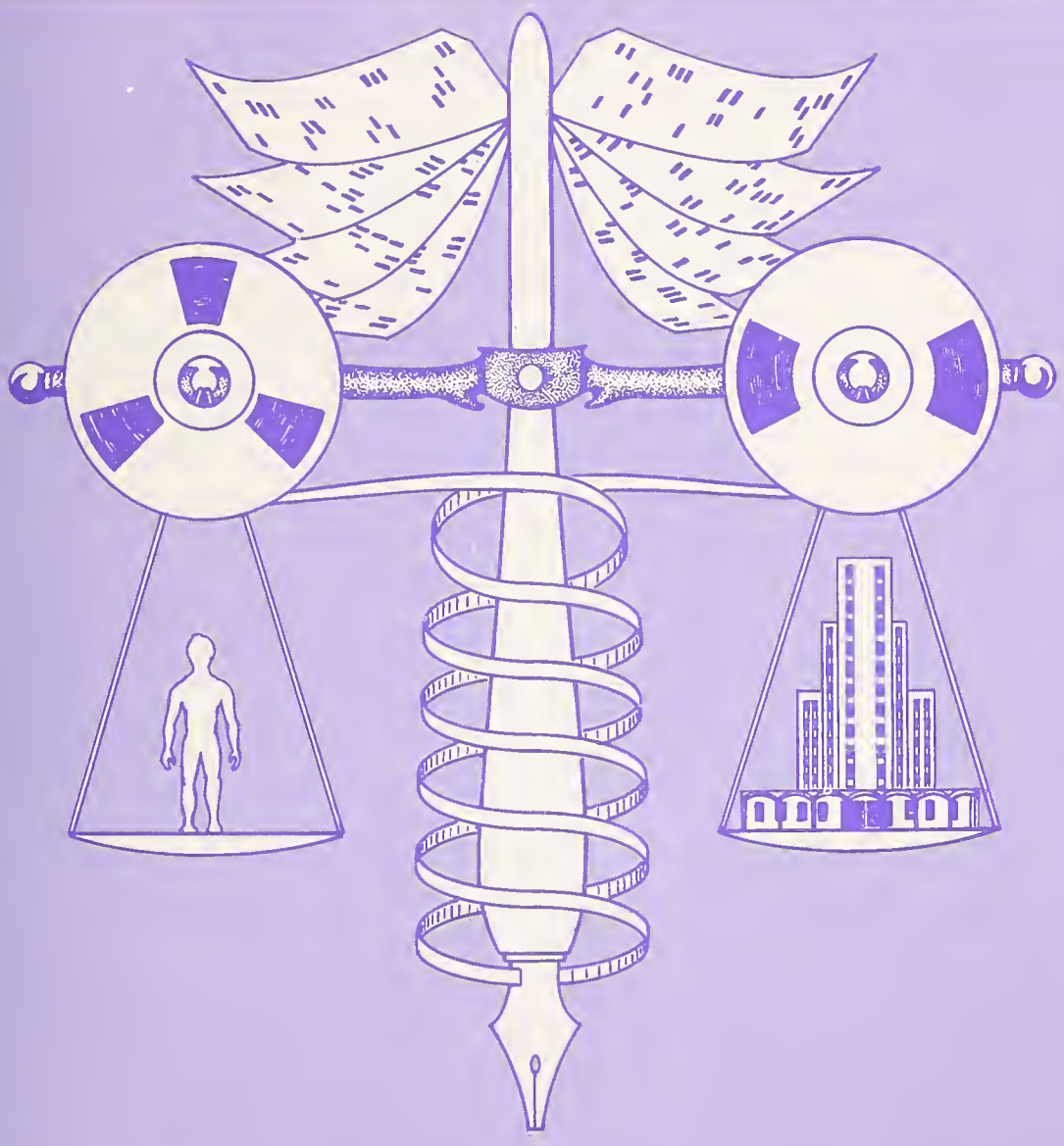
NBS SPECIAL PUBLICATION 469

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards



A Policy Analysis of Citizen Rights Issues in Health Data Systems

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. It is published in two sections, available separately:

• **Physics and Chemistry (Section A)**
Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

• **Mathematical Sciences (Section B)**
Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $9.45; Foreign, $11.85.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints and supplements available from ACS, 1155 Sixteenth St. N.W., Wash. D. C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington D.C. 20402.*

Order **following** *NBS publications—NBSIR's and FIPS from the National Technical Information Services Springfield, Va. 22161.*

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services (Springfield, Va. 22161) in paper copy or microfiche form.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service. A literature survey issued biweekly. Annual subscription: Domestic, $20.00; Foreign, $25.00.

Liquified Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00

Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.

A Policy Analysis of Citizen Rights Issues in Health Data Systems

Alan F. Westin

Department of Public Law and Government
Columbia University
New York, New York 10027

with

Florence Isbell, Editor

Sponsored by the
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Elliot L. Richardson, Secretary
Edward O. Vetter, Under Secretary
Dr. Betsy Ancker-Johnson, Assistant Secretary for Science and Technology
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued January 1977

Library of Congress Catalog Card Number: 77-600001
National Bureau of Standards Special Publication 469
Nat. Bur. Stand. (U.S.), Spec. Publ. 469, 48 pages (Jan. 1977)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1977

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.10:469). Stock No. 003-003-01730-2 Price $1.05
(Add 25 percent additional for other than U.S. mailing).

FOREWORD

The use of computers to automate the information handling and record-keeping activities of Government and private organizations has brought the benefits of speed and efficiency to these operations. But it has also brought concerns for privacy stemming from the desire of individuals to control the collection of information about themselves and to exercise some measure of control over the use of that information.

Consideration of this basic issue -- how to utilize the benefits of technology while preserving individual rights -- has led to public policy regulating the use of personal information in credit reporting and Federal record-keeping.

Medical record-keeping is an area of special concern and broad impact for the development of sound public policy respecting privacy rights. Computer technology applied to medical records offers promising benefits of increased efficiency and improved health care. Advances in computer and communications technology could enable doctors in remote areas to have ready access to relevant information. The analytic power of the computer could be used in medical diagnosis. Medical research could be advanced through computer analysis of existing medical records.

However, this is a sensitive area where privacy concerns are strong. The National Bureau of Standards has sponsored this study of the privacy issues in medical record-keeping to advance understanding of the attendant privacy problems and their possible solution. This report, Computers, Health Records and Citizen Rights, is the result of a two-year research effort directed by Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University. Dr. Westin is the co-author of Databanks in a Free Society, the landmark study of computers and privacy.

We offer Dr. Westin's recommendations to the health care and medical community for their consideration with the hope that these recommendations will help them develop policies that assure the protection of individual privacy rights. As the first thorough investigation of privacy issues in one sector of American society with sector-specific recommendations, it should provide helpful insights and a model methodology for studying privacy concerns in other areas. Towards this end, NBS and the Privacy Protection Study Commission are jointly sponsoring a follow-up study by Dr. Westin on personnel record-keeping practices.

Dr. Westin's study deserves wide review and careful consideration.

Ruth M. Davis

Ruth M. Davis, Ph.D.
Director
Institute for Computer
Sciences and Technology

PREFACE

This booklet is a condensation of the final report of the Project on Medical Records and Citizen Rights, sponsored by the Institute for Computer Sciences and Technology, National Bureau of Standards, United States Department of Commerce. The full project report, titled Computers, Health Records, and Citizen Rights, is available from the U. S. Government Printing Office. 1/

The project's work was done between the summer of 1974 and April of 1976, by a small, interdisciplinary team headed by Alan F. Westin, Professor of Public Law and Government, Columbia University. 2/ It represents the first in a series of NBS-sponsored studies into the effects of the increasing use of computers on citizen rights' interests in various fields of government and private record-keeping about individuals. Health care was chosen for the first study for several major reasons: the key role that health records play in virtually every person's life history; the growing use of computers in health care delivery and payments mechanisms; the likely enactment of a national health insurance program and a new health data network in the near future; and the expanding public debates over goals and alternatives for our national health care system, including rights to be exercised by patients and the public.

The study had three objectives. First, it would describe the pre-computer baseline of record-keeping practices and citizen-rights rules in the various sectors of American health care. Second, it would describe how computers were being used and identify the effects they were having on the content and uses of health records. Finally, the study would analyze public debates over computer uses and citizen rights in the health field, note parallel developments in other democratic nations, and identify those principles of good practice and possible policy actions that would best assure the observance of citizen rights in health-data practices, especially in automated data systems.

To accomplish these objectives, the project examined relevant published literature from the field of medicine and health, computing, law, and the social sciences. Interviewers, health professionals, and various public-interest groups (representing consumers, civil liberties, and minority-rights concerns). Materials were collected about several hundred health-care organizations, health insurers, and government health agencies currently using computers to process personal records. Six of these were selected for on-site visits and the writing of in-depth profiles. (The six are Los Angeles County Medical Center; Martin Luther King Jr. Health Center, New York City; Kaiser Permanente Health Plan, Oakland, California; the U.S. Indian Health Service; Mutual of Omaha Insurance Company; and the Multi-State Psychiatric Information System, Rockland County, New York.) Materials on confidentiality policies were also solicited from over 70 professional organizations in the health field.

A Draft Report of the project's findings and analysis was completed in July of 1975. This was reviewed at a conference of experts in September 1975, chaired by Dr. Vernon Wilson of Vanderbilt University. The Draft was also reviewed by mail by approximately 50 additional experts. On the basis of suggestions from these reviews, the Draft was completely rewritten and will be published by NBS in late 1976. Responsibility for the findings, policy analysis, and recommendations is solely that of the project director; no clearance of the final report was sought or required from the reviewers or the project sponsor.

The suggestion was made by several participants at the September 1975 review conference that it would be useful to prepare a condensed version of the final report that could be circulated widely among those reponsible for creating, managing, supervising, and judging newly-emerging health-data systems. This was done by project writer Florence Isbell and the director, and is presented here. We hope that it will help managers of health-care facilities, leaders of health organizations, government officials with oversight responsibilities in the health field, and leaders of citizen rights groups to focus on the increasingly important issues of information policy involved in the record-keeping aspects of our national health care system.

1/ NBS Monograph 157; SD Cat. No. C13.44:157

2/ Project members were: consultants: Michael A. Baker and George J. Annas; research assistants: Helene Toiv, Richard Silberberg, and Jamie Broder; administrative assistants: Lorene Cox and Florence A. Erickson; translations of foreign materials: Daniel Lufkin; typing: Barbara Delventhal; writer/editor: Florence Isbell.

CONTENTS

ABSTRACT

This is a condensation of the report "Computers, Health Records, and Citizen Rights" by Alan F. Westin, NBS Monograph 157, which investigates the impact of computers on citizen rights in the health record keeping area. Under Dr. Alan F. Westin's direction, from July of 1974 to April of 1976, a small interdisciplinary team did the following: (1) examined published literature from medicine and health, law, computing, and social science; (2) conducted interviews with major computer manufacturers, systems developers, health professionals and civil liberties, public interest, consumer, and minority-rights groups; (3) made on-site visits to six representative health-care organizations using computers to handle personal records; (4) corresponded with 70 organizations in the health field; and (5) subjected an initial draft report to review by a conference of experts in September 1975 and subsequently by about 50 outside reviewers. The findings of this investigation were then combined into this four-part report. Part One describes the world of medical data and citizen rights within the framework of three zones--primary health care (by health professionals), service payers and health care reviewers and social uses of health data (such as in employment, life insurance, and welfare); Part Two treats patterns of computerization in health care in each of the above zones; Part Three contains the profiles of the six health-care organizations that were studied in depth; and Part Four analyzes the impact of computerization on personal health records, presents comparisons with six other democratic nations, and states 12 recommended management principles for health care data systems. The full report also contains a 28 page bibliography and 12 appendices with support documents and information.

Key Words: Citizen rights; computers, confidentiality; data systems; health records; information policy; management principles; medical records; privacy; record-keeping practices; security

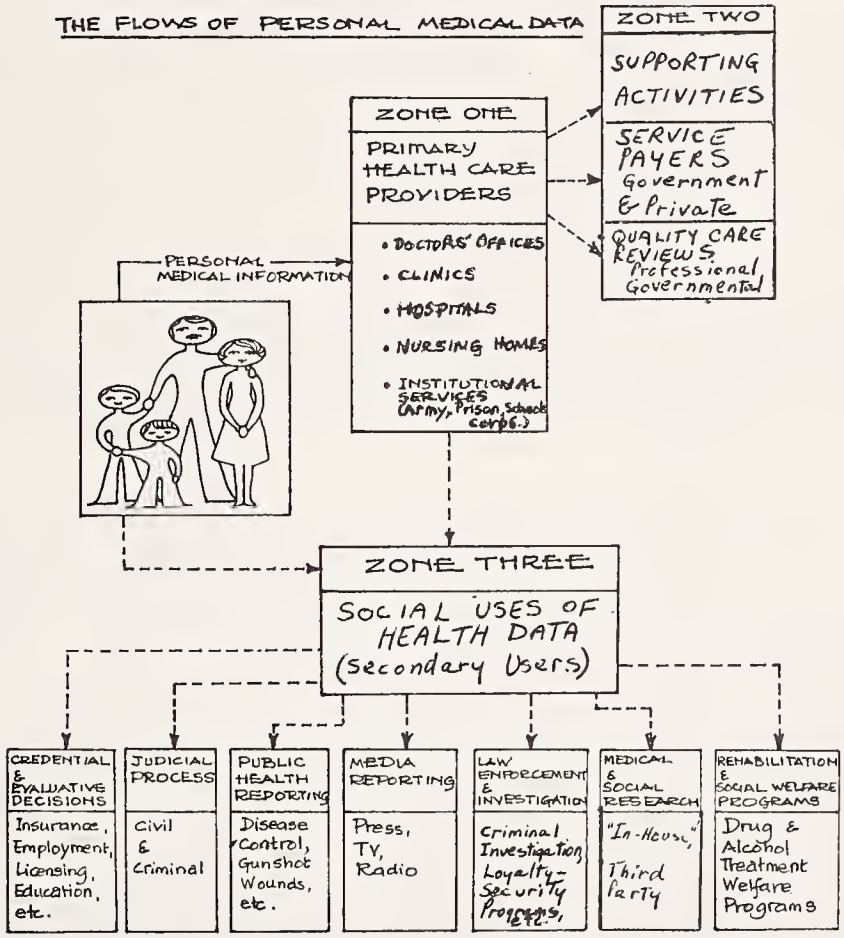
PART ONE: THE WORLD OF MEDICAL DATA AND CITIZEN RIGHTS

To measure the impact of computerization on health records and citizen rights, we need to establish how medical records and health data have been collected and circulated in American society as computer use moved into health care. We also need to see what laws and definitions of citizen rights were operating in manual record keeping, both in theory and practice, as well as the kinds of disputes over medical data and civil liberties claims that were already arising when computerization arrived. For the purposes of summarizing this background, we have divided health care and medical record-keeping into three zones:

Zone 1 - Primary Health Care - Medical records created when a patient seeks care from a health professional-personal physician, hospital, health center or clinic, college infirmary, company doctor, etc.

Zone 2 - Supporting Activities - The use of medical records by those who pay for medical care, both private insurance companies and government programs like Medicare and Medicaid; and by private groups and government agencies that review medical records to determine whether hospitals and other health care providers are in fact delivering the health care for which they are being reimbursed.

Zone 3 -Social Users of Health Data - The use of medical records in the non-medical world in determining whether individuals are eligible for licensing, employment, education, life insurance, credit, welfare and other government benefits, and when they are subject to investigation by law enforcement agencies.



ZONE 1. PRIMARY HEALTH CARE

Record-Keeping in Doctors Offices and in Hospitals

Privacy - It is almost universally accepted that full disclosure by the patient to the health care provider is necessary for accurate diagnosis and effective treatment, and few objections are raised about the circulation of patient information among medical personnel directly involved in patient care. But in many hospitals, people not involved in patient care have access to the patient's record -- including

medical students, social workers, financial workers, researchers, etc. The very presence of the patient in the hospital is taken to imply consent for this access often without the patient knowing of it. Typically, the patient's record follows him or her to the ward and may be seen by all the nurses, ward workers and cleaning staff on all three shifts. Most hospitals do not make a conscious effort to foster an atmosphere of patient privacy; hospital staffs take it for granted that patients will constantly be physically exposed to their ward-mates and to the staff in their most intimate functions, and sharing of intimate medical information with peripheral hospital staff must be seen in this context.

Not all hospitals send the full medical record with the patient, nor do they keep the full record in one place. In some institutions, financial information is kept by the billing office, drug orders by the pharmacy department, consent forms and other materials by the social service department, etc. And in some institutions, this information is kept in a central file and duplicated by other departments. In many large hospitals, central medical records are handled by medical record administrators, of whom more than 11,000 now work full time at supervising medical record rooms.

Two chronic problems of hospital record keeping are record retrieval and extracting needed information from the record when and if it is retrieved. Often, physicians request prior records for only a portion of their patients because (a) they are not delivered as fast as needed; (b) identification problems sometimes result in the wrong record being delivered; and (c) the needed information must be laboriously extracted from a thick patient file, and thus is unusable. These difficulties provide a strong impetus for computerization of patient records.

Psychiatric Hospital Records - The medical portion of general hospital records may relate only to the illnesses being treated. But psychiatric hospital records are likely to be all inclusive because every aspect of the patient's life is deemed relevant to his treatment. Also, many staff members may contribute to the patient's record, according to sociologists Kai Erikson and Daniel Gilberton, "physicians, psychologists, social workers, nurses, occupational therapists, aides, clerks..."

In some psychiatric hospital records, case histories and certain test results are stored in the central record room or in a locked closet off the ward, while day-to-day files such as medication records and doctors orders are kept in the patient's ward. While the patient's privacy is protected by keeping sensitive material off the ward where students, aides and janitors roam at will, the partitioning of records draws status lines through the hospital staff that adversely affects both morale and the treatment of the patient. In any case, Erikson and Gilberton suggest that when records are stuffed with nursing notes and social work interviews, clinicians do not have the time to read them.

Two related privacy questions are stirring debate: What should be recorded and how long it should be kept. For example, should "emotional distress" letters, written to justify abortions before they were declared legal, remain permanently in hospital files? Or to put the question in a larger framework, when can patients have records that are alleged to be inaccurate, incomplete, biased, or based on outmoded social or ethical standards expunged, and by what procedures?

Confidentiality - From the Hippocratic Oath to the present, the doctrine of confidentiality is the cornerstone of the doctor-patient relationship, promulgated to assure the patient that the information volunteered will go no further than the health professional to whom it is confided. But in fact, the doctrine of confidentiality of medical records often is forced to give way to other public interests -- medical, legal or social. While 38 states have laws that "privilege" the patient's communications to doctors (in recognition of the tradition of confidentiality) it is not widely understood how limited this "privilege" is, and how many exceptions to it the statutory law recognizes. "Privilege" means that the person to whom information is given is forbidden by law from disclosing the information in a courtroom without the consent of the person who provided it. Thus it applies only to judicial proceedings, and belongs only to the patient, not to the health care provider. The physician-patient privilege is not recognized in common law (those laws made by judicial decisions and not by legislative enactment of statutes) so it exists only in those 38 states with privilege statutes.

The best way of understanding the limits of the physician-patient privilege is to list some of the exceptions in state statutes or court decisions by which

health professionals are either permitted or required to reveal medical information about their patients:

1. Public reporting laws: Physicians and hospitals are required to report births and deaths, infectious or communicable diseases, deliberately inflicted wounds, child abuse and industrial accidents to the appropriate local, state and federal agencies.

2. Consent of the patient: The patient may bring medical records into court when suing a doctor or hospital for malpractice, or in a personal injury suit against a third party. As noted, the privilege belongs to the patient, not the doctor. But often, the patient's consent to release medical information is not at all clear-cut:

General or Blanket Consent - Patients are often asked to sign authorizations permitting hospitals to release medical information about them to anyone the hospital thinks should have it, with no restriction placed on the amount or the relevance of the material thus released. Under this blanket consent, hospitals may make records available to many non-medical sources, such as law enforcement agencies. But the most common and unquestioned dissemination of both hospital and physician-patient records is to insurance payers, both private and governmental.

Hospital patient records are also used for both internal and outside quality care review. Where federal money is disbursed for health care, such as in Medicaid or Medicare, federal regulations require the establishment of Professional Standards Review Organizations (PSRO) to monitor facilities and professional services. The Joint Commission on Hospital Accreditation, a private, standard-setting organization, requires that records contain "sufficient information to justify the diagnosis and warrant the treatment and end results." Local and state agencies also conduct hospital reviews, including surveys of record-keeping practices.

Partial Consent - Some courts have held that when the patient gives consent to partial disclosure of his record, he has "waived" his right to protection against disclosure of the full record.

3. Best Interests of the Patient: Courts usually give physicians wide latitude in making disclosures that physicians believe are in the patient's best interests. Telling an employer of a patient's condition that would disqualify him for certain work (e.g. a pilot being subject to blackouts) would probably be covered by this doctrine. Some state laws, too, make an exception to confidentiality statutes on this ground.

4. Supervening Interests of Society: Courts have decided that a doctor has the right to reveal to private third parties as much information about a patient as is necessary for others to protect themselves against infection or other dangers stemming from the patient's condition.

5. Public's Right to Know: This exception applies mainly to the press, and generally relates to newsworthy individuals. Generally hospitals give out only minimal information about a patient's condition unless they have express permission to release more, as when a politican authorizes release of detailed information to avoid damaging public speculation. But police spokesmen sometimes release information about newsworthy criminal suspects against their wishes. A separate question is raised by the release of medical information in the press obtained in a questionable or illegal manner, as in the case several years ago of a New York newspaper which revealed that a local district attorney was hospitalized for lung cancer, when his office said it was fatigue. The Post defended using stolen hospital records by saying the electorate had a right to know the facts, since the district attorney was running for re-election. Court decisions seem to indicate that so long as the press did not themselves commit a crime in obtaining the information, they can publish it if there is a legitimate public interest in it.

6. The Judicial Process: In general, the common law principle is that the courtroom is an arena for discovery of the truth, and confidential communications should not be beyond the court's reach. Retention of the privilege was the most controversial item in the new Federal Rules of Evidence, adopted in 1975. Initial versions eliminated the privilege entirely, but the final version leaves it to individual courts to decide where there is not a governing state confidentiality

statute. A special privilege was retained, however, for communications between psychotherapist and patient.

Where courts have found a breach of patient confidentiality, the cases have generally not turned on that breach alone. The key element has usually been publication, generally accompanied by a photograph of the patient, that could be construed as commercial exploitation or advertising. In such cases, sometimes the suit is against the publisher, and not the physician or other health care provider.

The law relating to confidentiality of medical records is very sparse. Few patients bring lawsuits because they usually have no way of knowing who has had access to their records. Even when they learn this, they may decide they cannot afford litigation. Furthermore a lawsuit means public notice of the very information they wish to keep confidential. Most important is that the prospects of such litigation are not encouraging. There is no reported U.S. case in which a physician or hospital has ever had to pay money damages for breach of confidentiality (although some publications have paid damages.)

Eliminating Exceptions by Statute - One way to increase the confidentiality of medical records is to protect them specifically by statute. An example is the New York statute to protect the Multi-State Information System for Psychiatric Patient Records, at Rockland State Hospital. The statute specifically declares that these records are "confidential and not subject to examination in the courts or by agencies of this state....are not public records....and not subject to subpoena in any court or before any tribunal or administrative agency."

Patient Access to Medical Records - The movement to promote policies and laws to give patients access to their medical records is part of a growing consumer movement to place limits on the power of institutions to determine important aspects of peoples' lives. Especially now, when medical records are wisely shared with insurance, law enforcement and government agencies, and employers, it is often crucial for patients to know what is being recorded and to correct inaccuracies that may affect education, career advancement, or government benefits.

This drive for patient access runs head on into the traditional view of most health professionals that they alone can decide what patients should know about their records, that access might lead patients to become confused or anxious, and that this undermines good medical care. Some observers have suggested a compromise between these two positions: that patients be given access to any part of their record that may be disseminated to others, while those parts of the record that reflect the physician's "thinking out loud" or subjective impressions could be kept from the patient.

Summary of the Law on Access: A few states have special statutes enabling patients to view and copy their hospital medical records. (Some statutes limit this right to the patient's attorney or authorized representative.) The most liberal of these is the Massachusetts statute which gives patients an absolute right of access during and after their hospital stay. But, in fact, a recent test showed that a majority of hospitals in Massachusetts disregarded the statute and continued to deny access, and patients in Massachusetts had to bring suit to enforce it. Where there is no special access statute, the only way a patient can get information from his medical record is to bring suit against the doctor or hospital (usually alleging malpractice) and getting a court order, a situation that an HEW commission in 1973 found to increase "the incidence of unnecessary malpractice litigation."

Health professionals frequently deny patient access to medical records on the ground that they are the property of the physician or hospital. However, appellate courts have held that while the physician or hospital may own the paper on which the record is written, the patient's interest in the information is so vital that he does have a right to it. In the few access cases litigated, courts have given patients access to their general hospital records, although there has been less unanimity about access to mental hospital records.

The access statutes do not cover private physicians' offices, perhaps because legislatures are uncertain of their power to interfere with a physician's private practice. There are no recorded cases directly on this point.

Thus, for the present, in states with access statutes, patients must often sue to enforce them. In states without them, state hospital regulations permit hospitals to adopt restrictive access procedures. As a practical matter then, hospitals can control access in most cases in which the patient is not willing to sue. However, the doctor-patient relationship is undergoing change, and certain legal trends point to greater patient access in the future. Passage of the Federal Privacy Act of 1974 and of fair information practices acts in five states has created a general right of access to records held by federal or state agencies in those jurisdictions, including medical records. In addition, state courts are recognizing that before giving consent to medical treatment, a patient needs information about his/her condition, the recommended treatment and its probable results; that the patient has a right to self-determination, to refuse treatment or to choose between alternative treatments. These decisions are as yet the rule in only a few states, but they indicate the trend of some courts to see the doctor-patient relationship as a decision-making partnership instead of a medical monopoly.

While these courts have taken a giant step in recognizing patient autonomy, physicians may still invoke the "therapeutic privilege" to deny access, that is, that a disclosure need not be made when a doctor can prove that it would so seriously upset the patient that he/she would not be able to weigh the risks of the treatment. While this tends to limit the doctrine of patient access, it does put the burden on the doctor to prove the need for the therapeutic privilege, and the presumption in the ordinary case is that the patient has the right to be fully informed.

Medical Records for Special Populations: Large groups of people have medical care provided because of their special relationship to a particular institution: the armed forces for servicemen; correctional institutions for inmates; some corporations for employees; and some colleges for students. Under these circumstances, health care providers are not usually independent practitioners but employees of the institution. Sometimes this dual loyalty serves both the patient and the institution well; sometimes the conflict in loyalty undermines the doctor-patient relationship and interferes with the delivery of medical care. Some of the special aspects of medical record-keeping in these special situations are noted below.

Correctional Institutions: Medical care, like every aspect of institutional life, is subordinate to security. This means that patient interviews are rarely conducted in private, but in the presence of guards and other inmates. At daily sick calls, medical records are not kept on patients with minor illnesses; prisoners with medical emergencies are generally taken to outside hospitals for treatment. Copies of these outside medical records are given to the institution's administrators. Sometimes they are not even given to its medical staff.

Most medical information about prisoners is placed in their general records by non-medical personnel, primarily guards, but sometimes by prison teachers, social workers or the clerical staff. Inmates' records are routinely available to prison personnel. They play a role in cell assignments (those diagnosed by guards as homosexuals, drug addicts, and malingerers, for example, may be confined to cells with no privileges), and they are used by disciplinary boards within the institution and by parole boards.

Armed Forces: Military law does not recognize the physician-patient privilege and doctors are expected to report any patients' confidences that might affect performance to the command. Such information may be used to determine a serviceman's fitness for promotion or whether or not they should be summoned before an administrative hearing board or court-martialed. Where a court-martial is a possibility, military physicians are required to give the patient an "Article 31" warning, which is the military version of the Fifth Amendment that what he says may be used against him, although the formal language of Article 31 need not be used.

Until March, 1974, Separation Program Numbers were affixed to general or honorable discharge papers which, unbeknownst to the veteran, were codes known to employers and others which frequently signified derogatory information, much of it medical information. There were codes, among other things, for homosexuality, psychiatric disorders, bedwetting, VD, alcoholism, drug abuse, obesity, and so on.

Employment: Most corporations provide limited direct medical care to their employees, generally clinics for handling accidents or health emergencies. Virtually all corporations provide group health insurance coverage to their workers. This generates problems when the employer or his employees processing health insurance

benefits learn about sensitive health conditions of the individual, and make employment decisions on that basis. There are also problems when the employer releases information obtained from such health insurance records to third parties -- other employers, life insurance investigators, etc.

Colleges: A survey of 165 American colleges revealed that the great majority do not routinely inform parents of medical treatment unless the student is seriously ill, or hospitalized, or makes a suicide attempt. When the student himself seeks treatment the majority do not inform the school administration without the student's consent unless the student is very ill, or his condition poses a danger to himself or others. However, when the administration refers the student to the mental health service, the majority of schools inform the student at the outset that a report will be made to the dean.

The great majority of schools state they would reveal no information to outside organizations without student consent. However, this may include the routine or blanket consent students give upon admission or when they sign an insurance, licensing or employment application. Thirteen American universities, including Berkeley and Harvard, refuse psychiatric information to outside agencies even with student consent, a position more protective of confidentiality than that of the American College Health Association, which would permit disclosure to draft boards, insurance companies, prospective employers, the armed forces and the FBI, on the ground that under some circumstances "....refusing to give information will be seriously damaging to a former patient."

ZONE 2. SUPPORTING ACTIVITIES

As already noted, medical records in Zone 2 are used for two separate but related purposes. The first is for the payment of health care for individuals eligible for medical benefits under government programs or private insurance plans. The second is to monitor the costs and quality of care given to these patients.

Private Service Payers

Where private insurance companies are providing individual health insurance coverage, there are two aspects of that coverage that call for scrutiny of personal medical information: eligibility and payment of claims. As to eligibility, it must be remembered that health insurance coverage is by no means universal or evenly distributed in the population. Some 20 million Americans have no coverage at all. Some families are covered for only a small fraction of their medical bills, while others have policies with a full range of medical services. All of this means that for every individual covered by private insurance, decisions must be made as to his or her eligibility, what rate he or she should pay, and whether the particular policy covers the benefits claimed.

As long as there is no system of universal health insurance, accompanied by universal eligibility, private insurers will continue to make eligibility decisions. What civil liberties and consumer groups are questioning are the methods used to make such decisions, particularly the role played by outside investigative firms. Some long-standing complaints have been rectified by the passage in 1970 of the Fair Credit Reporting Act, which requires insurance companies who use outside investigative firms to inform applicants of the investigation. The investigating firm must discuss the applicant's report with him or her if requested, although they are not required to show it or to provide a copy. However, medical information does not have to be discussed with the applicant. A Senate bill, introduced in 1975, would end this exception, and would also disclose the sources of investigative reports It would provide advance notice to consumers when a report is being made on them for employment purposes. Most important, it would require specific consent, rather than blanket consent for the release of medical information, whether to a commerical reporting agency or the insurance company.

It is in the payment of claims however, that the major issues arise and they largely concern the confidentiality of personal medical data. Most private health insurance is not of individuals, but of employee groups. Our study collected many incidents in which sensitive medical conditions were disclosed to employers by health insurance firms, sometimes on the assumption that employers were entitled to know because they paid all or part of the premiums; sometimes because the initial claims processing was handled by the employer; sometimes because the medical claims unit of the personnel department considered it appropriate to inform management of medical conditions being claimed. Where government security clearances are involved, some

employers pass on insurance company reports containing sensitive medical information to government agencies.

Demands for the entire medical record by insurance payers are another source of complaint from doctors, and the complaint arises mostly where the doctors and hospitals are reimbursed for their services, rather than when patients are reimbursed for their medical expenses. For example, Mutual of Omaha, which does reimburse the patient directly, investigates "doubtful" eligibility thoroughly, but states that most investigations of claims are made only to establish that the loss is covered within the framework of the policy provision. By contrast, Blue Cross, which reimburses doctors, has an elaborate three-level system for reviewing claims, and when the claim fails to clear the automatic reimbursement of the first level, further information about the record, and sometimes the whole patient record is requested. Special scrutiny is given to conditions that call for long treatment where the outcome cannot be predicted, which is characteristic of psychiatric illnesses, because such conditions are prime possibilities for fraud -- for drawing out treatment and exaggerating the amount of care given to increase the amount of reimbursement.

Most observers agree that part of the skyrocketing costs of medical care can be laid to doctors who are defrauding service payers -- governmental and private -- and that careful investigation of claims is therefore essential, including examination of the patient's entire record. Many doctors, however, feel that demands for detailed and sensitive information (which is often irrelevant to settling claims) inhibit patients' willingness to confide necessary information to their doctors, can result in patients refusing treatment, and are insufficiently secured against unauthorized access within and outside the insurance payer's office.

This mounting concern about the confidentiality of service payer's medical records is leading them to re-evaluate their procedures. The National Association of Blue Shield Plans adopted new guidelines in 1975, restricting access to "the least number of people necessary" within Blue Cross, setting up training programs emphasizing confidentiality, and limiting information requests to only "those data necessary to adjudicate a claim....If the Plan needs only a discharge summary.... it should not ask the hospital or physician for the entire record...."

Government Payers

The government provides payment for health care for millions of Americans, including the 21 million Americans over 65 covered by Medicare, special health services (on a partly matching basis with the states) for the mentally retarded and blind, the emotionally disturbed, physically handicapped, alcoholics, drug addicts, children, and those eligible for disability benefits under Social Security. In addition, more than 60 million full time workers are covered under Workmen's Compensation laws.

Government agencies have two reasons for close scrutinization of individual medical records. In those programs, like Medicaid, where eligibility depends on financial need, the government tries to make certain that the individual's income is below the level set for participation. For all government programs in which reimbursement is made to the physician or the hospital and not the patient, the government's major concern is to make sure that the medical procedures it is paying for are in fact performed, and are in fact necessary in terms of sound medical practice. Misuse and fraud by health care providers is often cited as a major reason for the astronomical costs of government-funded medical programs.

Utilization Reviews and Quality Care Assurance

Utilization review is the system by which hospitals and outside monitoring agencies measure hospital facilities and procedures against established norms: overuse or underuse of facilities, length of hospital stay, patient-staff ratio, etc. Quality care assurance is the related examination of whether treatment prescribed for patients is appropriate and its delivery competent. Both kinds of reviews help hospitals plan the most efficient use of their facilities; help service payers control medical costs; and help assure patients good quality care under good physical conditions.

Utilization and quality care assurance are conducted on several, sometimes overlapping levels. Some hospitals conduct their own reviews against internal standards, and some compare themselves to other hospitals. Many hospitals use a private statistical review service, such as the Professional Activity Service, which extracts 50 or 60 items of information from patient records in almost a third of the largest general hospitals, against which individual hospitals can compare their own perfor-

mance. These reports are statistical and do not use identified patient data.

Among other reviewing agencies are the Joint Commission on Accreditation of Hospitals; state and local agencies responsible for sanitary, building, safety, and fire codes, as well as hospital costs; the Public Health Service, which prepares an annual Hospital Discharge Survey; and Blue Cross and Blue Shield, which set norms based on actuarial studies on lengths of stay, cost of physicians' services, and ancillary hospital services. Since the "Blues" can withhold reimbursement if they find their norms violated, this constitutes a powerful form of utilization and quality care review.

Professional Standards Review Organizations

By the early 1970's, the soaring costs of Medicaid and Medicare led Congress to create the Professional Standards Review Organization program (PSRO) to review the costs of medical care to detect fraud and misuse by health care providers. Under the legislation, 206 regional PSRO's are to be established, each to be run by a professional association which represents a substantial proportion of the physicians in each area.

The PSRO's functions are to pre-certify particular hospitals for Medicaid and Medicare patients and then to provide regular re-certification. They must also review the quality of care within the institutions to determine whether particular tests, procedures or operations are warranted, and whether they were delivered. In some cases, hospitals will conduct their own reviews, and the PSRO will then review the hospital's review. In other cases, the PSRO may assemble professionals to perform the review.

While specific administrative arrangements may vary in different PSRO's an example of one operation may be generally illustrative. Specially trained nurses will extract the patient data needed for certification forms. If the admission of a patient is certified, a projected length of stay will be decided upon, and patient and physician will be told that expenses will not be paid beyond that time unless the case is re-examined and re-certified. Difficult cases are referred to PSRO physicians.

When the patient is discharged, medical record technicians prepare a discharge summary, a copy of which is sent to PSRO. With the information, and occasionally from additional patient file information from the hospital, the PSRO will do medical evaluation studies, and maintain profiles on patients, physicians and institutions. When physicians depart substantially from the established norms for their region, they will be alerted to this. However, one of the PSRO's chief considerations is to avoid stigmatizing individual physicians by directing most of the educational efforts at the entire staff of the hospital. Only when a physician consistently violates PSRO guidelines, and has been afforded hearings at the state and national levels, and an appeal to the Secretary of HEW, can any censure of his or her activities be disclosed.

Since PSRO's became operational only on January 1, 1976, several aspects of their functions are still to be developed -- whether they will eventually replace totally the present Medicaid and Medicare evaluation programs; exactly what kind of materials they will collect for their reviews; what sort of patient-record review will become standardized; and whether PSRO will virtually compel the creation of state-wide or regional data banks.

Citizen Rights Issues in Zone 2

Within the past year or two, medical spokesmen and civil liberties groups have raised questions about whether the amount of detailed patient information sought by service payers is necessary for the functions performed; whether the data is secure against unauthorized third party access; and why identified patient data must be kept for long periods. This has led some insurers and care reviewers, along with medical societies and various government agencies to begin to explore such possibilities as removal of patient identifiers from many of the payment or review processes, whether notification to patients of how insurers process their claims and provision of rights of patient access should be required; and whether there are ways of lessening the amount of sensitive personal data required in payment for psychiatric treatment or stigmatizing conditions.

What is being reexamined, however, is the procedure for limiting and protecting the information supplied, and not the legitimate need for identified patient information. Any health care system -- public or private -- must know who the patients

are in order to pay for their care and to guarantee that such care meets professional standards at a reasonable cost.

ZONE 3. SOCIAL USES OF PERSONAL MEDICAL DATA

The survey that follows traces how organizations not directly providing health care, or paying for it, or monitoring it, obtain personal medical information and how this information is used.

Credential and Evaluative Decisions

Life Insurance: A quarter of the life insurance policies in force are on a group basis and require no health information from the applicant. Most of the others require at least a check with the Medical Information Bureau,* an industry-run medical information pool, in which 700 member life insurance companies contribute reports of "insurance related" medical conditions. MIB maintains files on 11 million individuals and handles 19 million requests for information, returning over 500,000 reports with adverse medical or other information. In addition to coded information covering hereditary diseases, TB, and mental disorders in the insurance applicant's family, the coded reports cover all major infectious diseases, alcoholism, drug dependency and injuries. Until recently, codes for "reckless driving," sexual deviance, social maladjustments and financial status were included, but MIB no longer requires member firms to report such information.

In 1974, after years of pressure from consumer groups and Congress, MIB adopted new rules to bring it into conformity with the Fair Credit Reporting Act. The applicant is told by the insurance company that information about him may be submitted to MIB; life insurance companies must obtain authorization from the applicant before the company is permitted to query the MIB computer; and they are also told that they may have access to the information about them and that inaccuracies can be corrected.

For deciding about larger policies or more "questionable" policies, a fuller investigation may be made. In 1972, almost 8 million life insurance investigative reports were completed by Retail Credit and similar firms.

Automobile Insurance: All states require individuals who own cars to carry liability insurance. This has resulted in a complex system of "assigned risks" which guarantees everyone at least a minimum of automobile insurance, but at higher rates. A 1974 study by an agency of HUD showed, however, that 20% of the nation's drivers are not covered by insurance, and that 3.3 of the 4.0 million drivers in "assigned risk" pools were "clean" -- that is, they had not had an accident within three years. The study concluded that age, geographical location, race, claims history and driving violations are more important than health reasons in placing applicants into the assigned risk category.

Employment: Health standards, like other criteria, follow the law of supply and demand in the labor market. The more plentiful the labor supply, the more rigid the health criteria become. Sometimes the health standards set by employers are not related to reducing absenteeism, increasing worker performance or keeping group health premiums low, but appear to be an exercise in selectivity for its own sake. Studies show discrimination by employers against those with mild, non job-related conditions, and widespread discrimination against those receiving, or who have in the past received, psychiatric treatment.

The importance of health information in employment decisions is demonstrated by the extent to which employers seek it. In addition to the employment application form, employers receive health information from company and private physicians, from insurance claims or the insurance carrier, from previous employers, from military separation papers and from investigative reports by private firms and government security agencies.

As to government security checks, "full field" investigations are normally made only for higher government posts or where there are national security considerations, but some government agencies order them for insignificant jobs when they get information that the applicant has had psychotherapy or may be a homosexual. Government investigators often interview school and private psychiatrists in order to gauge the "mental stability" of applicants.

---

* Medical Information Bureau is abbreviated as MIB in this document.

As noted earlier, for many years the U.S. military services included code numbers on veterans' discharge papers that labelled them with one or more derogatory "medical" terms. While the services have promised to stop this, veterans must affirmatively request their discharge papers to be changed to omit these codes. Since most veterans probably still do not know the meaning of the numbers, hundreds of thousands of them are still having this adverse information disseminated to employers.

As we have already noted employers get health information on their employees through group health insurance claims, either directly from the insurer, or when the company personnel department monitors claims.

In 1970, Retail Credit Corporation completed more than one million reports on job applicants and candidates for promotion. Where there is health information in such reports it comes from former employers, neighbors, personal references and workman's compensation files.

Maintaining Medical Records in Health Hazardous Industries

An entirely different problem of medical records in employment is that posed by workers exposed to occupational substances -- such as asbestos and vinyl chloride -- which are thought to cause cancer and which may not surface until 20 years after exposure. In these cases, management sought to conceal the relationship between the substances and the disease, and thus many companies kept no health records at all. Even where records were kept, in compliance with the Occupational Health and Safety Act, the exposed workers and their representatives were often refused access to them.

Licensing: All states have some licensed occupations for which the health of applicants is deemed relevant. Those who deal with the public -- barbers, nurses, hospital workers, food handlers, etc. -- are required to be free of communicable diseases. In New York and Michigan taxi drivers are checked through state fingerprint files to see if they have ever been patients in state or county mental institutions.

Licensing of drivers requires applicants to submit medical information about themselves -- ranging from information about vision, as in most states, to a detailed listing of ten medical conditions in Maryland, the presence of any one of which requires a physician's certificate describing diagnosis, prognosis and medication prescribed.

The Judicial Process

We have already noted some of the statutory exceptions to the privilege doctrine permit physicians to testify on patient information confided to them. In addition, all state privilege statutes have exceptions for criminal proceedings so that medical testimony and medical information can be introduced, i.e. a defendant's narcotics addiction to provide motivation for a robbery, a previous commitment to a mental institution to support an insanity plea, etc.

In civil commitment proceedings, a court-appointed psychiatrist may draw upon hospital records or personal observation to supplement a complaint from police or family members. Medical records are also introduced into quasi-judicial proceedings such as disability hearings, probation hearings and workmen's compensation reviews.

Among the concerns of health providers about the growing use of medical records in court are: fear that the doctor-patient relationship will be undermined by therapists testifying about their patients; concern that medical testimony is required for "frivolous" reasons, such as to support a purely pro forma charge of "mental cruelty" in a divorce proceeding; the lack of specificity in medical records subpoenas, sometimes requiring copying of the entire record instead of just the relevant portions; and, especially in psychiatric cases, concern that patients are not in a position to give truly informed consent to their therapists' testimony because of their mental condition. Physicians are also concerned about their own privacy in malpractice suits, fearing that adverse findings of internal reviews by their colleagues will be exposed in court which, they argue, would disrupt the voluntary cooperation of physicians with essential evaluation committees; this view is disputed by consumer advocates who feel that patients have a right to know when a physician is censured by colleagues.

The Media

In general only limited medical information is formally released to the media by hospitals, which follow the guidelines for confidentiality and public release promulgated by the American Hospital Association. However, reporters often get their information from tipsters on hospital staffs, military records and the Veterans Administration information.

Criminal suspects, state mental patients, prisoners and welfare clients complain about the release of their medical records to the press, in some instances by prison psychiatrists, by the Veterans Administration, and by police officers.

Law Enforcement

Patients' medical records are a natural resource and temptation to law enforcement officers seeking information on missing persons, drug abusers, illegal aliens, criminal suspects thought to have psychiatric problems, etc. In some states, the law specifically provides that the police may get certain kinds of information from medical files - prescriptions for narcotics, for example. In many states, the law is not clear, and this allows law enforcement officers to inspect medical files with little resistance.

While official hospital policy may prohibit releasing confidential information to law enforcement agencies, it is usually done anyway, as illustrated by a study of Philadelphia hospitals. This revealed that personal medical information was shared regularly with the District Attorney's office (which turned it over to the police), with Selective Service Boards, and with federal agents, despite specific guidelines to the contrary. Drug rehabilitation clinics are also likely targets for police investigation as the case of People v. Newman in 1973 illustrates. A lower court ruled that the Director of a Methadone Clinic had to turn over photographs of black male patients between the ages of 21 and 35 to the police after a witness to a killing said she believed she had seen the killer in the waiting room of the clinic. The appellate court reversed, on the ground that the clinic was specifically covered by the federal Comprehensive Drug Abuse and Control Act, which protects clinic patients and their records from identification and subpoena.

While our society accepts a certain amount of law enforcement access to confidential medical records, it is not clear at what point this access becomes an intolerable intrusion on citizen rights. If the decision is for more tightly controlled records, then the most direct way to secure it is by specific legislation such as the Comprehensive Drug law cited above.

Medical Research

A great deal of medical research requires identified records on research subjects because the medical treatment of specific individuals is being followed in a clinical setting, or because specific individuals are being followed over long periods of time. This research sometimes involves civil liberties issues: the problem of informed consent, as when 840 women were injected with a hormone, without their knowledge, and which 20 years later was found to produce a high incidence of cancer in their female children; or when a group of terminally ill patients were injected with live cancer cells without their knowledge; the problem of truly voluntary consent, raised when prisoners are "encouraged" to "volunteer" in the testing of new drugs; the question of the propriety of withholding treatment from patients for research purposes, as in the experiment in which a group of men was allowed to go for many years without treatment for syphilis so researchers could study the disease.

The problems just outlined have raised more concerns than those of confidentiality, access and privacy of records with which this report is concerned. However, one mental health clinic did refuse to participate in a study of the demography of mental patients because its psychotherapists believed that the very collection of data from mentally-ill patients is an invasion of their privacy and interferes with therapy. In a Baltimore study of the relationship between the XYY chromosome factor and juvenile delinquency, suggestions were made in the press that the research data should be turned over to juvenile courts, thus raising confidentiality problems. (The suggestion was vetoed and the research remained confidential.) In another XYY study in Boston, a patient advocate group demanded records access for parents of the boys being tested, raising difficult questions because the researchers themselves were not sure of what the findings meant. They did agree to give parents a general explanation of the aims of the project.

School Health Records

The long standing practice of keeping comprehensive files on students is being influenced by two modern trends affecting their medical content. The first is that public schools have become places for the provision of public medical care, including immunizations, hearing and eye tests, screening for sickle cell anemia, and other various childhood conditions. The second is the increased frequency with which the medical model is applied to learning and behavior difficulties. Medical labels such as "dyslexia," "hyperkinetic," "minimal brain dysfunction" are being applied to children, often by non-medical staff, and such labelling is often put into the student's central record from which it may be disseminated to colleges, law enforcement agencies, or employers. Thus, the chief citizen rights issues raised by the use of school medical records are: 1) The possible inaccuracy of medical information placed in the student's file; 2) The stigmatizing or prejudicial effect that this information -- whether accurate or inaccurate -- may have on the student; and 3) The possible inability of the school system to prevent health information from being released outside the school.

Such concerns were a chief impetus to the passage of the federal Family Educational Rights and Privacy Act, which gives parents and students over 18 access to elementary and secondary school records. The Act has been in effect less than a year, and it is too early yet to tell how widely access will be sought and what effect it will have on how school records are kept.

Rehabilitation and Social Welfare Programs

Among the many government rehabilitative and social welfare programs involving medical records, two -- treatment of drug addicts and child abuse registries -- illustrate the controversy about how such records should be handled.

Drug Addict Centers: It is estimated that between 30 to 50% of all crime is drug-related, so it is not surprising that law enforcement agencies are interested in the records kept on addicts at drug treatment centers. On the other hand, medical experts stress that drug addiction can only be cured through medical treatment, that an important part of that treatment is the confidential relationship between therapist and addict, and that this would be destroyed if those who seek help were identified to the police. Failure to keep its promises of confidentiality is cited as the chief reason for the failure of the Armed Services massive effort to treat military drug abusers, and the same lack of confidentiality, or lack of clarity about confidentiality, prevails in civilian programs. Methadone clinic directors report constant pressure for identified patient records from state and local agencies, with the threat that needed funding will be cut off for non-compliance.

Child Abuse Registries: Recent estimates that one American child in 500 dies of child abuse have led to the passage of child-abuse reporting statutes in every state, and the establishment of central child-abuse registries in 30 states, to which any person may report a suspected case of child abuse. Most of the central registry legislation does not deal with the questions of access by accused parents or guardians, or the confidentiality of the material in the registers. There is no barrier to these registries being shared with law enforcement agencies, the courts, welfare departments, etc. Only seven states impose varying degrees of confidentiality, and only New York allows access by parents and deletion of undocumented charges from the registry. A further concern is that the registries serve to stigmatize the parents, often by unsubstantiated gossip, but the state has little capacity, once it gets information on child abuse, to provide care for the abused child or counselling for the abusing parents.

Conclusions: Zone 3 uses of medical data raise the sharpest clash between society's interest in protecting medical confidentiality and its interest in a wide variety of other important functions, both governmental and private. In each area, a rational case could be made for the exceptions to the normal rules of medical confidentiality, and some of these exceptions have been embodied in the statutory and the common law. These legally sanctioned exceptions tend to legitimate other exceptions which have developed as a matter of organizational practice.

However, two recent social forces are bringing these exceptions into question. The first is the movement creating outspoken constituencies for racial and sex equality, cultural and sexual diversity, and the rights of stigmatized groups such as ex-mental patients, women seeking abortions, etc. These groups view the use of

health criteria as a device to penalize non-conforming social behavior, by denying them opportunities for employment, education, credit, government benefits, etc.

The second is the deepening distrust of government that marks our era, with part of this distrust being disbelief that the government is either willing or able to protect confidentiality. Any discussion of the secondary uses of personal medical data must recognize that this public distrust -- greatly exacerbated by Watergate -- underlies the growing discussion of whether existing laws and controls over medical data uses are sufficiently protective of citizen rights.

PART TWO: ENTER THE COMPUTER

Computerization in health care is expanding in response to the same stimuli that affect other sectors of American society; rising demands for private and government services; demands for faster data transmission; heavily increased paperwork stemming from such transactional demands; rising cost of clerical labor; and increased government reporting requirements to satisfy social accountability. A dramatic example of the escalating demand for services is the increase in hospital admissions: 10 million in 1940 to 35 million in 1974. This increase, plus record-keeping requirements for insurance reimbursement, quality care reporting, and health-planning, create an enormous, ever-increasing data-handling operation. Hospital studies estimate that from 25% to 40% of hospital activity is spent in collecting, recording, communicating, and reporting medical information.

Trends in computerization in health care follow the overall trends in organizational automation within the past fifteen to twenty years. The basic pattern has been for automation to move first into financial activities (payroll, accounts receivable, etc.) where the data is of a highly routine, fixed character. The next stage is to automate large-volume, frequently used files containing data on clients and customers that is easily abbreviated and "objective." Then, many organizations moved in the 1970's into automation of more narrative, specialized files, often in the hope that more sophisticated computerization would assist complex decision-making. Recent years have also seen efforts by some organizations to develop multi-file databanks to provide comprehensive information systems for management.

COMPUTERIZATION IN ZONE ONE

Doctors' Offices

By far the most common computer application for doctors' offices is billing and accounting, sometimes with office-administration and claims-reporting "hung onto" these systems. Much of this computer use is by contract with outside firms specializing in medical data processing (some sponsored by local or state medical societies) or with general data-processing service firms. Where such outside firms are used, the spread of personal medical information to service bureau employees can raise confidentiality problems. The very fact that a well known person has visited a particular practitioner (a psychotherapist, for example) can be highly sensitive. Beyond this, some service bureaus do put substantive information on their statements as part of the standardized "billing package." While service bureaus recognize that confidentiality is vital to their business success, some celebrated breaches of security in business data processing have taken place in the past decade, and the movement of personal medical data to outside processing firms poses new risks to confidentiality.

In a few hundred situations, doctors have moved beyond billing and into automation of patient records in an effort to achieve comprehensiveness. Compared with the "jot-it-down-on-a-5-by-8-card" method, legible only to the doctor, automated records now produce detailed personal histories that can be read by all the personnel in the office. They can also be used as an evidentiary resource for insurance companies, workman's compensation investigators and others involved in civil litigation.

Between 1971 and 1974, HEW funded an experiment in computer applications in 13 doctors' offices which included automated medical history, diagnostic consultation, patient education, and family health planning and administrative services. At the end of the project, 4 physicians said they would continue computerization at their own expense; some of the others liked the system but could not afford to continue it, while the rest did not find the system particularly helpful.

Medical and computer spokesmen expect computer use in doctors' offices to increase slowly but steadily in the next five years. They cite increased exposure of physicians to hospital computers, the trend toward group rather than solo practice and, possibly most important, the rapid price decline in computer services, especially as minicomputers become increasingly available.

Hospitals and Health Centers

According to a 1974 survey by the American Hospital Association, virtually every hospital has computerized some aspects of its operations, the majority through purchase of outside computer services, and the minority (about one-fourth) through in-house computer. Size of the hospital is the determinative factor in in-house computer use.

The survey results reflect the general pattern of computer use found by a National Academy of Sciences study on computer use in business, government and associational activity, published in 1972. Three kinds of computerizing organizations were identified there. The first is the leading-edge user, willing to try ambitious, innovative computer applications, even those involving basic organizational changes. Some of these organizations are able to show cost-effective operations, while others are satisfied with the enhanced prestige as pioneers. The second type -- the majority -- is the mainstream user, who is willing to wait until new equipment and applications are proved by others. The third is the low user, who does some computerized data processing, but because of small size, lack of resources, fear of reaction by customers or subjects, or resistance of their own employees, limits its applications to payroll personnel, and administrative reporting programs.

For those hospitals which are leading-edge users, automation of patient records has changed the nature of the patient's file. Formerly, manual record-keeping was hit-or-miss, and while there were lots of documents in the record, they were often in disarray, without index or summary. Now, while the character of information in automated patient records is not different from before, the automated personal data are being more systematically collected, more fully recorded and more centralized in permanent files. From a health care standpoint, this is one of the most desirable features of automation -- patient records are full, up-to-date, easily understood, and linked together from various departments and previous episodes. From a civil liberties standpoint, however, this means that medical and paramedical personnel with access to a facility's computerized files now have more detailed social and medical histories than in the typical manual system, except for psychiatric facilities. In addition, computerization facilitates (and is sometimes intended to facilitate) sending some automated patient data to service payers, quality care reviewers, public health agencies, welfare and rehabilitation programs, etc. The more hospital data are automated, the easier, cheaper and more rapidly Zone 2 and 3 organizations can call for highly detailed information. This means that these records will require not just the observance of traditional standards of confidentiality (uneven as those have been) but new definitions of legal and public policy boundaries for data-sharing and the creation of monitoring and enforcement machinery to police these boundaries.

In noting some of the changes that automation brings to patient records, and in the discussion below on some of the specific citizen rights problems of computerization, it would be easy to conclude that computerization of hospital records must inevitably exacerbate violations of citizen rights. But this is far from the case. Much more important than computer technology in emphasizing or ignoring citizen rights are the attitudes and practices of hospital administrators, both of which are usually carried over from the manual record era. The profiles in our main report, of four primary care centers amply illustrate this.

1. Los Angeles County Medical Center is a large county facility primarily serving the urban poor and minority groups of East Los Angeles. It is an average or "mainstream" computer user, with a project to automate medical records in a databank to improve patient care. The profile shows that the factors which shape basic citizen rights policy are the pressure on the Center to recover costs, leading to an emphasis on collecting extensive personal data; the Center's cooperative relations with local government and police officials seeking patient data; and a "ghetto-crisis" medicine that has no place for such "luxuries" as giving patients access to records or obtaining truly informed consent before releasing patient information. Computer use at the Center incorporates these basic problems and reactive policies. The report concludes that it would take a combination of new patient-rights legislation and reorientation of staff resources and priorities to install significantly greater citizen rights in the Center's operations, and that this will not take place any sooner -- or later -- as a result of the Center's plans for further computerization.

2. The Dr. Martin Luther King Jr. Health Center is a federally-funded, private facility providing ambulatory care in a high-poverty area of the South Bronx, in New York City; it supplies comprehensive, family-centered health care to approximately 40,000 registered patients, with a staff of 450. Computer use has been of the "mainstream" variety, but this Center's emphasis on the health-team approach to care, its heavy use of community people in staff and decision-making, and its innovative policies and practices as to patient rights presents a fusion of computer technology and citizen rights that is very different from that of Los Angeles Medical Center, even allowing for the differences between acute and ambulatory care. The report regarded as exemplary the King Center's philosophy that machines must facilitate rather than weaken the Center's basic commitment to patient dignity and social advocacy.

3. The Kaiser Permanente Medical Care Program offers the experience of a five-year, "leading-edge" project on computerized patient records in the Oakland-San Francisco area, which was aimed at eventually creating a "hospital information system." As a pre-paid medical plan that is both medical provider and insurer, Kaiser serves primarily middle class and unionized workers, and its health care has been excellent. It gave careful and effective attention to citizen rights in the Oakland project, especially as to access controls over patient data stored in the computer system. The federal grant to Kaiser was not renewed in 1973, and while the report discusses the different explanations for this withdrawal of funds, the treatment of the Kaiser project underscores the uncertainty of funding and organizational problems that face leading-edge projects in the hospital field today.

4. The U.S. Indian Health Service operates an advanced health information systems project in Tucson, Arizona that maintains integrated, on-line medical records for approximately 10-12 thousand Papago Indians in Southern Arizona. Though this has helped greatly with some of the special problems of record-keeping raised by an itinerant patient population, and has generated excellent administrative reports, the computer project has not been able to do much about the desperate medical condition of American Indians in Arizona and elsewhere and the glaring inadequacy of federal funds and facilities being provided to cope with these health problems; in fact, the improved reporting only highlights the problems more sharply. The study found that the Indian Health Service has been sensitive to special Indian attitudes on privacy but that problems of confidentiality of records and issues of patient access remain. These are now being addressed under the new provisions of the Federal Privacy Act of 1974, and the report notes some of the initial problems that have arisen in implementing those policies in the Indian Health Service.

Among the existing problems being transferred to computerized records is what should be recorded and for how long. We have already touched on this in manual records in connection with the psychiatric-need letters written by doctors to justify abortions before the 1972 Supreme Court ruling legalizing them. A computer example comes from a pediatrician in a large metropolitan hospital, who finds computerized records "incalculably valuable" for information retrieval but who hesitates to record information about illicit drug use, pregnancy, truancy, etc., because of their availability to anyone on the computer. If such stigmatizing information were not preserved in the files of the primary health provider, the problems of ancillary or secondary uses would be eliminated or greatly lessened. Another privacy matter is whether a given automated system has informed patients that their medical data is being automated, and how it will be used.

Future Prospects for Hospital Computerization

Although hospitals have not used computers as extensively as many other industries, marketing studies are highly optimistic about their future use. One study predicts that hospital computer sales, which were $156 million in 1974, will rise to $380 million by 1979. Other computer industry and medical spokesmen predict more innovative uses in the future, including completely computerized patient medical records. However, some experts are not so sanguine. They believe that computerization will be inhibited by the lack of a conceptual model of information priorities and uses in the hospital, a model that could be generally accepted by doctors, other health professionals and by patients, not just by health care planners, hospital business managers, and data processing technicians. These dissenters believe that even the infusion of large amounts of money for developing hospital information systems -- something that was not present in the 1965-1975 decade -- would not lead to significant breakthroughs in the near future.

One of the reasons for this divergence of predictions about future computer use by hospitals is the lack of agreement about their current value and cost-effectiveness. This uncertainty is reflected in our two profiles of leading-edge hospital/health center users, Kaiser-Permanente and the Indian Health Service. At Kaiser, staff and outside evaluators judge the computerization of patient records to be strongly worthwhile in promoting better medical care. In spite of this, the federal grants to support innovative computerization have been withdrawn. While Kaiser will continue pioneering in computerization, its advances will by no means be along steady and predictable lines. In the Indian Health Service, too, computerization is enthusiastically supported by staff, but both staff and agency supervisors recognize that first priority must be given to the basic problems of Indian health, nutrition, and sanitation, and no funds to expand the system have been appropriated for the coming three years.

Other Primary Health Service: As noted in Part One, direct health care is provided in a number of institutional settings - colleges, corporate medical programs, prisons, etc., and automation has spread deeply into some of them. We looked at one of these, college health services, to show how automation is being used in such facilities.

Most colleges provide health services ranging from in-patient emergency care to regular medical, dental and mental health services. Typically, colleges obtain a medical history from the entering student, maintain regular student-patient records, and keep special files on drug and alcohol abuse, birth control and abortions, suicide episodes, psychiatric care and similar matters. Of particular interest from our standpoint are the commercial firms that market automated medical questionnaires, of which Medical Datamation is an example. It offers a 964-item self-administered questionnaire that, in addition to a complete medical history, covers demographics, family background, eating, exercise, smoking, alcohol, information or help wanted by the student, and a word association checklist relating to emotions. From this automated data, a medical database report, a problem list, a problem-monitoring report and statistical summaries are generated. The issues raised by the use of such automated histories were summarized in a letter to us from a nurse who is serving on the privacy committee of a state medical records association: "First of all...any 'Yes' checked by the student... including such things as information requests for birth control..is placed on a problem list...What qualifies (this) as a 'problem area'?

"In addition, the Problem Monitoring Report strongly violates privacy and confidentiality...the student is not told that such reports will be compiled, nor...who will have access to the reports. The Monitoring Report could be particularly harmful in a student health service where often times non-professionals are employed, and who might disseminate the information to unauthorized persons..."

COMPUTERIZATION IN ZONE TWO

Service Payers

Our study describes in some detail the progress in automation by private service payers (who were heavy users of computerization from the start) and by government payers, who were low users in the 1955-1965 decade, but were forced by the enactment of Medicaid and Medicare into widespread and rapid computerization. Computer use by service payers has not changed the citizens' rights problems we summarized in Part One. The crucial aspect of these problems remains unclear policy definition: what is a private or government employer, or other third party, entitled to know about specific medical conditions of an insurance subscriber or claimant? Should no information at all be given to third parties on the ground that health insurance firms receive this information solely for purposes of claims adjudication? Or should group policyholders, whether government or private, be entitled to learn of certain health conditions that could impair their employees' job performance or make them ineligible for promotion or security clearances, etc. The point to underscore is that this is a gray area today in terms of law and policy, not one on which law is clear and is being willfully violated.

But while leakages of confidential medical data have so far involved manual forms, not computer printouts, there is little doubt that patient and doctor confidence in automated service payment will be impaired if imprecise policies prevail. The issue is whether service payers should be collecting and/or retaining as much data as they do now, given the fact that many medical and civil liberties commentators feel they are not limiting its circulation sufficiently in manual forms.

Another trend in automating service-payment mechanisms over the past two decades has been the entry of data processing firms as intermediaries under Medicare and Medicaid, and in various utilization review projects. Among the best known of these is the Electronic Data Systems Company (EDS) owned by H. Ross Perot, which processed over 75 million health insurance claims in 1973 for various state agencies and Blue Shield/Blue Cross plans. This lodges personal medical data still further away from the ethical constraints of the primary-care providers or the Blues (which the medical and hospital professions themselves developed and still influence directly). Given the sometimes politicized character of the contracting process that has awarded claims-data contracts to commercial firms, and the essentiatly non-medical character of these "data shops," attention clearly needs to be paid to how well protected these files are today in legal status and how securely they are kept in fact.

Utilization Reviews and Quality Care Assurance

In order to assist hospitals to administer and evaluate their care, a number of medical data systems have been developed in recent decades that collect trend information from data supplied by private payers or government agencies, or from hospital patients' records. Such data allow institutions to compare patterns of care, outcome, costs, use of space, etc. The most important aspect of such activity is the hospital discharge data system for in-patient care activity, of which the largest is the Professional Activity Study (PAS), a non-profit corporation sponsored, among others, by the American Hospital Association. Participating hospitals send PAS a set of basic data about each patient discharged which is abstracted from medical records, including patient demographics (age, sex, race), dates of hospital stay, diagnoses, operations, consultations, outcome, source of payment, drugs, etc. The basic confidentiality principle of the PAS system, which now has almost 110 million individual case abstracts stored in its automated database, is that the hospital retains the identity of the patient and the doctor, with PAS' case abstract filed only by a number. The participating hospital, knowing the number, can have reports prepared on the basis of various groupings of case abstracts, but PAS and other participating hospitals cannot obtain a case abstract with the name of the patient or doctor on it.

As to quality care assurance, we have already noted the creation of PSROs in Part One. It remains to be seen how computerization will develop in them -- whether through existing intermediaries, or through state-wide data banks. Proposed PSRO guidelines prohibit one centralized databank system, provide confidentiality safeguards, and call for patient access, but it is not yet clear how the system will operate in practice.

We did two profiles in the Zone 2 area:

1. The Multi-State Information System (MSIS) is an automated information system containing records on about 400,000 mental patients. It serves both administrative and research purposes for participating institutions (primarily state and private mental health facilities in the Northeast) and the research activities of the developer and manager of the system, the Information Sciences Division of Rockland Research Institute, a state facility in Orangeburg, New York. As a support activity for primary care providers, we put MSIS in our Zone 2 category. MSIS has pioneered in securing a special state statute to safeguard the confidentiality of the sensitive psychiatric data that it stores. But it has also been the target of considerable attack because it creates a new type of centralized, regional databank of identified psychiatric information, separate from and in addition to the records kept in the participating mental facilities. The report notes that providing strong safeguards for such regional and national information systems containing special medical data is especially important in the post-Watergate climate of public concern over government abuse of confidential records.

2. Mutual of Omaha is a profit-making, multi-line insurer which is not only the largest provider of private health insurance in the United States but also an advanced computer user. The report traces the citizen rights issues involved in underwriting decisions and claims investigation at Mutual, and the compliance of the firm with important protective legislation such as the Fair Credit Reporting Act and the Federal Privacy Act (the latter because Mutual is a fiscal intermediary under several federal health-payment programs). The report found that Mutual's use of computers has followed rather than altered its basic confidentiality policies, has probably enhanced the security of subscriber data, and has not interfered with Mutual's compliance with federal laws. The key issues of citizen rights facing Mutual and all other health insurers, the study noted, are issues of social policy, such as how far American society will insist upon socializing certain risks (insurance of homosexuals, forbidding "objective" but racially-based standards, etc.) and thereby alter the collection and use of per-

sonal data that now support industry practices in these areas.

COMPUTERIZATION IN ZONE THREE

Zone 3 -- welfare, law enforcement, credit, life and auto insurance, etc. -- is so variegated and diverse that we did not attempt to describe its computerization patterns. (The impact of such computerization on citizen rights, however, is analyzed in a later chapter.) What we selected for description in Zone 3, because of its special importance, are important trends in computerization by government health agencies. Only a few key facts are needed to illuminate the citizen rights issues posed by such computerization. For example, in a recent survey of computerization by state mental health authorities, out of 47 jurisdictions replying, half said that they stored personally-identified psychiatric information in their files, either by name or Social Security number; this was primarily for the purpose of controlling costs, with special emphasis on scrutinizing elibility for government services. The survey found that "requesting affirmative authorization for computerizing a patient's personal psychiatric information is virtually non-existant." Such state health-agency automation practices raise citizen rights issues as to whether such records need to be collected and stored by the state with personal identifiers. When these are attached, this raises the issue of informed patient consent to such use; notice of and control over access to the records by other state agencies (licensing, welfare, law enforcement, etc.) and rights of inspection by patients as to what is put in about them.

One important development in federal law deserves mention -- the 1975 Health Planning and Resources Development Act. This calls for the creation in 1976 of 200 health service areas, each to be administered by a health service agency that can be a private body, a non-profit organization, or a public agency, depending on local option. The act requires each of these 200 agencies to create a database on the health status of its residents, an inventory of local health facilities and personnel, the effect of the current system on health, and other aspects of the local profile. Guidelines still have to be released by HEW, but the issues of identified versus statistical data, controls over data circulation, and patient access clearly lie ahead.

Conclusion

Computerization of personal medical information has been haphazard and not according to thoughtfully conceived plans. In the same way, policy as to citizen rights issues is developing on an ad hoc basis, carrying over for the most part the same practices pursued with manual records. Given the more detailed, more centralized, more permanent, and more easily transmitted character of computerized medical records, the flawed procedures and policies currently employed with respect to manual records threaten to be even more seriously inadequate to the computer era.

1. ASSESSING THE COMPUTER'S IMPACT ON CITIZEN RIGHTS

Several significant social forces affect our perceptions of the impact of computerization on citizen rights, and these will provide the framework for our analysis:

The Computer Seen as an Instrument of Continuing Discrimination

Stigmatized groups in our society (homosexuals, physically handicapped, ex-drug or alcohol abusers, women who have abortions, person receiving psychiatric treatment, etc.) are struggling for an equal competitive opportunity with others in winning credit, employment, housing, government benefits, and other societal rewards. They object to organizations conducting intrusive personal investigations which will identify them as having these stigmatized conditions, blocking them from benefits which, they claim, should not depend upon such irrelevant criteria. On the other hand, where society has recognized a group's right to equal treatment and sets enforcement mechanisms to provide affirmative or even compensatory treatment, as in the case of women, blacks, and other racial minorities, the recording of a condition is generally accepted as a practical necessity. Thus, the complaint of groups which have not yet won recognition of their rights to legal and social equality is really less one of invasion of privacy than it is a tactic in their struggle to win recognition of the fact that their condition ought to be immaterial to the decisions being made. Such groups have as much concern with manual records as with computerized data, but they see computerization as accelerating discrimination because it is more systematic, more extensive, more centralized, more easily disseminated, and more permanent.

Skepticism about "Data-Based Government Social Programs"

The gap between the health data collected by computers for socially useful programs and the actual delivery of such programs is all too common, as our profile of the Indian Health Service graphically illustrates. The IHS computer generated all sorts of statistical studies showing the relationship between poor housing and poor health; the role that poor nutrition played in certain diseases, what diseases were most prevalent; what medical equipment and staff was lacking, etc. But while the computer continues to churn out these studies, the housing of the Indians continues to deteriorate, the disease rate continues to climb, and the medical equipment and staff needed to meet Indian health needs is not being supplied. Our study documented similar examples throughout a wide range of government programs -- examples in which large numbers of citizens are asked to disclose sensitive personal information in order to help government make "rational" planning decisions. It should not surprise government officials that when such "rational" enterprises fail to behave rationally -- that is, to deliver what their announced objectives declare -- citizens will become increasingly disbelieving of the promises under which they are being persuaded to reveal personal data.

General Distrust of Government and the Watergate Fallout

If we were living in a time of high citizen respect for government and social institutions, skepticism about government promises might be regarded as a minor matter. From the 1930's to the 1960's, there was widespread acceptance that government authority was needed to end the Depression, wage World War II, carry out Great Society programs, and help insure racial and sexual equality. But this trust in government's efficacy to solve social problems has visibly eroded since the late 1960's. Conservative critics have attacked centralized big government and urged a return to decision making on state and local levels, as well as using private instead of public programs wherever possible. Many liberals have become disillusioned with the failure of government programs to ameliorate poverty, crime, racial inequities and other problems. Within both ideological camps, the failure of government programs has also led to doubts about using legal coercion to collect and store extensive personal information on behalf of programs which have had little positive effects.

All of this might still have remained at "normal" levels of American distrust of government had it not been for Watergate and the revelations following it -- revelations of how top officials breached Internal Revenue Service confidentiality, illegally opened personal mail, spied on political critics with illegal wiretapping, and resorted to burglaries and break-ins to secure confidential information. The illegal activities of the FBI, CIA, IRS, Post Office, and other agencies have convinced the average person that the label of "confidential" on any personal file held in government does not guarantee its security against the efforts of federal, state or local investigators to get information by overt or covert means. Thus, the call for personal data to carry out even the most laudatory government programs must - fairly or unfairly bear the burden of Watergate and post Watergate revelations.

Consumerism in the Health Care Field

One of the basic premises of consumerism is that people have a right to be truthfully and fully informed about the products and services offered to them. In the field of medical records, this is expressed in the demand that patients be given the right to examine the primary medical record and to know about any other uses made of it. The consumer's demand to know in order to make an informed "buyer's" choice about the nature, quality and consequences of health treatment matches the civil libertarian's insistence that access is vital to informed consent in the doctor-patient relationship, and the securing of due process whenever rights or opportunities are determined through use of medical information.

Other social forces and trends are also playing a role in creating the complex setting in which health computerization is taking place. Among these are the changing character of the law, which is beginning, through federal and state statutes and regulations, to provide some detailed guidelines for confidentiality and access; and a more realistic public understanding of the capabilities and limitations of computer technology.

But our major emphasis is that computerization of health data is unfolding in an atmosphere of considerable public mistrust over the motives, promises, practices and performance of government agencies, mixed with a rapidly growing public belief that citizens rights protections should be instituted by positive regulation before sensitive new data systems are implemented.

Analysing Potential Harm

In analysing the impact of computerization on citizen rights thus far, we will want to keep two observations in mind. First, most instances of harm done to individuals -- violations of confidentiality, refusals of access, etc. -- are still almost entirely confined to manual rather than computerized files, because manual files are the places where most detailed medical and health records are still being kept. Second, physical security for the computer and its programs is generally stricter and tighter than for manual records, and thus there is greater protection in computer systems against certain kinds of leakages and misuses. What we can conclude therefore, is that the main problem today in computerized health data systems is potential harm. What makes this potential harm so serious is the fact that the possibilities for misuse have not been taken into account and dealt with effectively by managers of computerized systems.

To develop our analysis of the impact of computerization, our study presented a series of incidents involving the creation or use of computerized records collected during the two years of our project. Each episode was related in detail, with comments on what it suggested about computerization and citizen rights. For the purposes of this brief summary, we will use only those episodes illustrating a major citizen rights question and state only the main problem raised.

Missouri State Division of Health: In June, 1974, the Missouri Division of Health ordered all Missouri hospitals, private and public, to provide easily identifiable patient discharge data, including demographics, marital status, source of payment, diagnosis, treatment, and physician's name. Failure to provide this information could lead to loss of the hospital's license to operate. The purpose of this order was to assist the department to "study the prevalence and control of disease in Missouri." This episode contains several elements typical of those arising with computerization: 1) The change from voluntary to mandatory compliance came because the computer made processing more information possible; 2) the need for computerization of identified patient data (rather than statistical data) for the purposes of disease control was not balanced convincingly against the rights of confidentiality of the patients; 3) the proposal to computerize identified data was not accompanied by any plan, regulation or draft legislation to prevent dissemination of identified data; particularly no attempt was made to secure legal protection of these records from the operation of Missouri's public information laws; 4) special concerns were raised because the identified computerized data might be sought by other state health or welfare agencies with compatible automated systems, or demanded by federal officials. Protests from the medical community were so strong that the demand for mandatory compliance was dropped.

Mental Health Computer Systems in Washington State and New York

Computer use by the mental health agencies of Washington and New York State was similar to the Missouri incident: the existence of a computer prompted the collection

of identified data; there was no well-demonstrated need for requiring identified data; and there were no accompanying legislation or regulation to safeguard identified data. However, the identified data required in these two systems went far beyond the identification-payer-diagnosis level: they required submission of the most sensitive and detailed data about each patient. Even if a need could be demonstrated for requiring some identified patient data for program planning and evaluation, questions would still be raised about how much and what kinds of data should be collected for such purposes. One aspect of the New York incident was that by law the information would be available to courts, service payers, missing persons bureaus and law enforcement agencies.

It is worth noting that in several episodes treated in the report, the organized protests of professional or civil liberties groups resulted in the project either being abandoned or modified. This illustrates the tendency of many government agencies to create new automated data systems without giving the people to be affected by them or the general public advance opportunity to make suggestions or call for changes in plans.

California Community Services Division and Washington State Department of Social and Health Services

Both of these incidents involved demands by the state for the agency to submit extensive, identified data on welfare clients, including such medical data as the unemployability of individuals because of mental disability, mental illness, drug dependency, pregnancy, etc. The purpose of requesting these data in both instances was to monitor welfare eligibility. Here, social workers refused to submit the data because o fears that sensitive personal information would be leaked to other government agencies.

The main purpose of computerization of welfare records is different from computerization in the previous examples and raises another difficult question. In the previous examples, a compelling case could be made that identified data was not necessary for program evaluation and utilization studies. But where the goal is welfare eligibility, identified data is obviously essential. The issue then becomes not whether or not to collect identified data, but how much and under what circumstances. Thus, the courts have ruled that in determining welfare eligibility the state may legitimately inquire as to how many members are in an applicant family and what their incomes are. However, the state may not conduct surprise nighttime visits to an applicant family to discover whether there is an "unauthorized" man living in the house (who might be supplying unreported income), since such visits violate constitutional rights of privacy.

Thus, the questions raised are: a) What limits are needed to assure that the information requested is relevant to the purpose, in this case, welfare eligibility; b) should these limits bar sensitive psychiatric data, especially since such data might be made available to other state agencies, e.g. law enforcement officials; c) do clients have the right to know that what they confide to a social worker will be sent to a central computer and made available to other state agencies?

Juvenile Justice Records

A number of states have computerized juvenile justice files, with materials taken from interview forms with counselors. Among the boxes to be checked on these forms are "schizoid," " latently psychotic", and similar brief phrases. Such terms call for professional diagnosis, but the counselors are not medical doctors or psychiatrists. These forms are available to court personnel, researchers, the FBI, the military and prospective employers, but not to the juvenile or his/her representative.

The questions raised by computerized juvenile records are: a) Does the shorthand term, fostered by computer coding, distort the diagnosis, even if it is an accurate one? Should such diagnoses be used when made by a non-professional? These questions are of particular concern because disclosure and recording of sensitive information about juveniles is encouraged in the widespread belief that juvenile records are either expunged or permanently sealed and therefore not available to other government agencies or private organizations. But in fact, juvenile arrests and/or convictions are often leaked to other local officials, and when they are reported to the FBI, they have been placed in regular criminal files and made available to a wide variety of "authorized" private and governmental agencies in the same way as adult arrest and conviction records.

Central Registries

Our study analyzed 8 types of state and county registries, including child abuse, drug prescriptions, abortions, foetal death, and drug abuse. All of them are based on the premise that a necessary step in dealing with serious social problems is to have identified information on the individuals suffering from or participating in the problem behavior. Much of the conflict over these registries stems from the lack of legislation or regulations limiting access by other government agencies. One of the registries we studied -- the Cleveland, Ohio registry for methadone patients - typifies the questions that they raise. The registry's purpose was to prevent individuals from enrolling in more than one program. But the data collected called for age, sex, educational level, employment history, criminal history, past history of drug use of all types, and other sensitive items not relevant to controlling duplicate enrollments. The Cleveland ACLU objected to these disclosure requirements as overbroad and conditioning a government benefit on the individual's willingness to surrender privacy. They also insisted that patients should have a right "to access and correct his file," which was not provided.

Much of the impetus for collecting full, identified information in such central registries flows from the example or, in cases of matching state-federal funds and administration, from the requirements of the federal government. In two instances, the governor of Massachusetts refused to submit identified drug-abuse data to federal registries, stating that Massachusetts would rather forego federal funds than comply. In both instances, the federal government agencies backed down, agreeing that identified information was not necessary and aggregate, statistical data would serve as well.

Computerized central registries organized around a single issue - child abuse, abortion, drug abuse, etc., - present in heightened form all of the problems we have previously catalogued. This is because they are, by their nature, government catch-alls. Some agencies with access (or seeking access) see them as invaluable for research; others for planning and utilization; others for providing social services; others for eligibility and avoiding duplication of benefits; and still others for law enforcement. The registries are created because there is general agreement that a difficult problem must be solved and that the first step is to identify those suffering from the problem; since computerization facilitates collection of such data, the move to central registries has been strongly accelereated in the past few years.

Although there is often public agreement that a central registry is a good idea, there is less agreement as to which of the above-listed purposes it should serve, usually because viewpoints differ as to the larger question of how the problem should be solved. As a result, such registries tend to collect all the data they can on a particular subject so they can serve each of them should the occasion arise. Such ill-defined goals often tend to be reflected in ill-defined limits as to the identification of individuals, the data to be collected, who contributes to the collection and rules for dissemination.

Texas Central Data Bank

In 1974, Texas announced that it was establishing a computer file that would pull together and record all the state "client" services. Each record would have name, Social Security number, race, birth date and other personal data, and a summary of state services being provided - health, mental health, rehabilitation, blindness, alcoholism, probation, welfare, higher education, retardation, youth services, and others. The purpose of the data bank was to eliminate duplicate applications, coordinate services, and improve planning and organization of social programs. The Texas ACLU and other groups protested that existing state and federal laws expressly protect the confidentiality of some of these services and that opening the index to state officials would violate that confidentiality.

When state officials noted that the individual's consent would be required before his/her name would be entered in the index, the ACLU countered that consent would rarely be voluntary. "What individual who had received services from a mental health clinic, or treated for alcoholism, or been confined in a youth facility, would freely consent to have this information float from agency to agency via computer?" In early 1975 Texas abandoned the data bank for lack of funds.

A similar multi-file data bank in Wisconsin drew fire from citizens rights groups. In response to these protests, the Wisconsin plan was modified to provide for separating individuals' names from special identification numbers, but even with this change,

the protesting groups felt that identification of individuals could be achieved without too much difficulty.

The central databank concept translates into reality the previously expressed fears of critics about uncontrolled dissemination of identified information from one government agency to another. The plans for the Texas and Wisconsin databanks highlight the citizen rights problems and deepen debates over confidentiality, adequacy of notice, consent, challenge and correction in such system.

In our discussion of the Mental Health Computer Systems, we touched on the public's role in planning state systems, but the process deserves to be further explicated here because it has special relevance for large, complicated multi-level data banks. What takes place is that first the databank is created; then protests arise from civil liberties groups and professional associations; then the government agency often tries to make some accommodation to the complaints, usually with limited success -- limited because the reforms are tacked on as an afterthought and are not really viewed by officials as an integral part of the system. Until such citizen rights considerations are included in the earliest planning for databanks, recognition given later will be regarded by critics -- rightly -- as something grudgingly granted, and distrust will greet even well-meaning efforts by government officials - as an afterthought -- to safeguard these systems properly.

In discussing the citizen rights problems connected with various computerized systems, we have focused primarily on lack of protections for confidentiality; less attention has been given to the individual's right of access. In only two incidents was access given equal weight or more weight than protests about confidentiality. While this conforms to patterns already established with manual health records, in the past few years there has been a growing consciousness that individuals do have a right of notice and access when records are collected and used to make governmental or consumer judgments about them. But in the cases of computerized health records we have been discussing, most of the individuals whose records are included are probably not aware of their existence. A right of access -- even if it were to be established -- would be meaningless unless accompanied by the right of notice, notice not only that the information was being recorded in the first instance, but being forwarded to a centralized data system, which would in turn forward the information to other state agencies. In this way the individual would know where his/her records are which might require correction or updating.

We noted when discussing manual records that the greater the dissemination of medical records that played an evaluative role - in employment, licensing, law enforcement, government benefits, etc. - the more important was the question of access with the opportunity to correct errors. Centralized computerization heightens this importance in direct proportion to its greater capacity to disseminate personal information to a broad variety of agencies and institutions.

Maryland Drug Abuse Administration

In March, 1974, the Baltimore press reported the following story. Some months previously, an informant had notified the Director of the Drug Abuse Administration that some employees of the agency had been using narcotics at "a party." As a result, the Director and other state officials decided to send an undercover state police agent into the Drug Abuse agency to pose as an employee. During the six weeks that he worked there, the undercover agent developed evidence that resulted in the arrest of several employees on charges of drug violations, including use of narcotics "at or near the drug abuse headquarters.

The threat posed by the presence of an undercover police agent to the security of the drug abuse registry and other confidential records kept at the agency caused a united protest by local and state drug treatment programs, medical groups, hospitals, and the Maryland ACLU. The program's director countered the protest by stating that the undercover agent had been given "specific instructions" not to have anything to do with this confidential data. This was not accepted as a satisfactory answer, and as a result of continuing protests, several significant changes in agency methods were made. Authority over record keeping was shifted to the agency's medical director, who announced that he was destroying all identified records for the past five years, and instituting a coding system for data to be sent to the state. These steps were hailed by the citizens groups as "protecting both privacy and rehabilitation." However, the question of whether police would be used in the future as undercover agents in drug programs and other sensitive social-rehabilitation programs was not addressed by state officials.

We have tried to avoid as far as possible the "what if?" approach to computerization and to confine our analysis to factual episodes. However, the placement of an undercover agent in the proximity of supposedly confidential files speaks to all the fears generated by the Nixon-White House plumbers, the burglary of Dr. Fielding's office in the Ellsberg affair, and the complex of issues raised by Watergate. It cannot help but evoke the question: What if the need were compelling enough -- say a threat to the President's life, or the danger of a mass terrorist bombing -- would any system, even one protected by special statute, be secure against encroachment by law enforcement officers? And if such special situations were held to justify law enforcement access, then who among state or federal health officials would have the power, the incentives, and the guts to deny access to law enforcement officials in other "special" situations as they arose?

The answer to these and other "what-if" questions lies first in the adoption of specific protective statutes and of special review bodies to pass on requests for exemptions or exceptions. But it also requires increasing public familiarity with the dangers as well as the benefits of computerization, increasing sensitivity of government health and social services officials, and persuading the courts to take a lead in defining and applying citizen rights concepts. The ways of fostering such attitudes will be discussed in the concluding section of this report.

The Medical Information Bureau

So far, we have confined our incidents to government computerization, which is where most public attention has been focused. But the problems of computerization are raised as well by some private organizations, as for example, the Medical Information Bureau (MIB), to which we alluded in Part I. As noted then, MIB receives information on life insurance applicants from its 700 member life insurance companies and stores data on some 11 million persons, on whom it reports to member companies on request. Consumer, civil liberties and Congressional spokesmen have been protesting some aspects of MIB's operations for the past ten years, although the general public, and especially individuals who might be denied life insurance or charged higher rates because of derogatory information supplied by it, were not generally aware of its existence.

The chief criticisms of MIB were: a) its collection and dissemination of "social data" (sexual behavior, finances, life style, mental "impairments" etc.); b) the lack of any provision for a person to inspect, challenge, and correct information in the record; c) the capacity of member life insurance firms to use MIB data for their accident, health and auto insurance lines, even though MIB rules said they should not do this. (It should be remembered that the Fair Credit Reporting Act of 1970 exempted medical data from its notification and access protections, and thus MIB is not covered by its requirements.)

MIB reacted slowly and defensively to these complaints. Only in August, 1974 did it stop collecting "social data" and after that, announced that insurance applicants would be told by MIB member firms that health data would be submitted to MIB and shared with other member firms. It then also initiated limited access, through request from MIB, to life insurance company, to "attending physician" who would then explain the file to the applicant. In response to criticism of this circuitous route, MIB in 1975 further broadened its access policies, although medical information would still have to be filtered through the individual's physician.

That MIB has made some changes is praiseworthy; but that it took agitation by critics for almost a decade to produce more organizational responsibility does not speak well for the life insurance industry, or for MIB, or for the public officials in the states where MIB is chartered (Connecticut) or has its files (Massachusetts), or for Congress, which ought to have written careful provisions for consumer rights in the MIB data bank when it enacted the Fair Credit Reporting Act.

A "Free Consent" Experiment

When government agencies computerize health and welfare client records, they often proceed on the assumption that the clients themselves are not worried about violations of the privacy of their records; this is mainly a case of overblown fears by self-appointed defenders. An interesting experiment testing this assumption was performed at a Community Mental Health Center in Georgia, starting in 1974 when Georgia required mental health clinics to send identified personal health data to the state. The experiment, designed by Dr. Catherine E. Rosen, Director of Research and Evaluation at the Northeast Georgia Community Mental Health Center, was conducted in two phases. In Phase I, clients were presented with a form written in standard

legalese asking their consent to have their identified records released to the state. (Illiterate clients had it read to them). Each of the 962 clients in the Center's four clinics signed the form. Compliance was 100%.

During Phase II, the same form was given to clients, but in two clinics, an additional statement, in simple English, was read to each client explaining the purpose of the form and what consent would mean. In these two clinics, with 109 patients, compliance was again 100%.

In the other two clinics, the simply-worded statement was also read, but it was followed by an additional statement:

> "If you do not sign this paper, this identifying information will not be sent into the state offices in the capitol, and will be kept only locally. In other words, if you don't sign, you will get the same services from us as if you did sign."

In one of the two clinics where the statement was read, compliance among 259 clients dropped to 41%. In the other, compliance among 105 clients dropped to 20%. The spontaneous remarks by clients presented with the "option" statement left no doubt about why they refused to sign. They were concerned that forwarding this information about them would adversely affect employment, or child custody, or would be put to some unknown harmful future use by government.

Dr. Rosen's study proves what civil libertarians have been asserting for years -- that millions of people do care about circulation of their personal data, and that their consent would not be freely obtained for many inadequately protected government data systems if they really had adequate notice or any choice of whether to consent or not.

OVERALL CONCLUSIONS ABOUT "COMPUTER IMPACT"

All the incidents we have presented in this chapter arose from Zone 2 or Zone 3 activities -- uses of computerized medical records or health data for utilization reviews or to make evaluative "non-medical" judgments about individuals. But the sources of the data in many such cases were computer files maintained by primary care providers in Zone 1, and thus collection and storage there has to be viewed in light of the demands for production of identified data being made by the Zone 2 and 3 activities.

Our analysis of these incidents suggests some almost painfully simple conclusions. Most computerized health data systems are being created or expanded without sufficient consultation in advance with groups representing citizen rights and doctor-patient interests, and without some kind of proceeding open to the general public. Most data systems lack sufficiently developed analyses of how much and what kind of identified personal data they really need to perform their function. Even when properly defined, most data systems fail to adopt sufficiently precise standards of confidentiality, controlling uses within the organization and releases of identified data to third parties. When it comes to rules for permitting patient access to their own records, extremely few computerized organizations have adopted procedures responsive to those patients who ask for and insist upon access.

Noting these general defects is not to say that there are no real problems of conflicting values or hard choices of social priority involved. Indeed there are, and that is what we will take up in our final chapter. But we approach this task of discussing alternative policies and making recommendations with the judgment that both citizen rights and effective use of computer resources require that we move away from ambiguous and ill-defined systems that leave people uncertain and fearful about their capacity to control the circulation of their medical and health data.

2. COMPUTER USE AND CITIZEN RIGHTS IN OTHER COUNTRIES

As a preliminary to considering policy alternatives, our project compared American developments with regard to medical automation and citizen rights with trends in other democratic nations. We found the same pattern of leading-edge systems, mainstream users and low level users as in the United States. However, leading-edge applications in most European nations began with a larger role for

government than in the United States, either through socialized medicine or a national health plan, and they therefore play a more direct role in funding and evaluating computer applications in health care. In addition, government agencies are often the direct manager of regional health data systems that maintain a record about the health of each resident in the region. Here the availability of official citizen identification numbers has played a major role.

Our project studied in detail developments in Great Britain, Canada, West Germany, Australia, France and Sweden. From this, we drew the following conclusions:

1. As in America, computers are playing a valuable role in increasing administrative efficiency and providing some improved patient services. But the problems that have inhibited greater use in the United States -- competition between medical and social priorities, professional resistance to technological experimentation, and lack of demonstrable cost effectiveness, have been duplicated in the nations we surveyed.

2. There is widespread theoretical agreement in the countries we studied that citizen rights in medical record keeping need to be protected. There is also agreement on the basic principles that would, if enacted, insure that protection: data systems should be limited to the information necessary and relevant to their functions; the public should be made aware of the existence of data systems and their operations; individuals should be notified when their personal records are stored in data systems and be told who will have access to them; individuals should be permitted to inspect their records and challenge their accuracy and completeness.

3. These countries have created different mechanisms to achieve protection of citizen rights goals, generally paralleling the way they deal with the larger records-and-privacy issues. One model is the Swedish Data Act and similar regulation in West Germany. In these two countries, automated personal data systems are officially licensed, and detailed regulation and continuing oversight are vested in regulatory boards or commissioners. Medical data is part of the total range of data systems covered by this licensing arrangement.

In Great Britain, proposed legislation would create a Data Protection Authority to insure privacy safeguards for the personal information that data systems contain. The legislation would mandate public notice of each data system's existence and purpose, limit dissemination and length of retention of records, and insure informed consent of the subject. A temporary Data Protection Authority has been appointed in Britain to work on privacy problems prior to the enactment of such national legislation.

In the other industrialized nations we studied, legislation to protect privacy has been recommended by parliamentary or special commissions. In some of these nations, Australia for example, specific safeguards for national health insurance data or data kept by primary care providers has been recommended and will probably be adopted separately from regulations covering non-medical data.

There is a common mood in the Western democracies about the need now to adopt privacy protections. As expressed by the French Minister of State and Interior: "For several years now, in France and abroad, legislative and regulatory programs have been proposed but rarely adopted. We have now arrived at the state where we have to choose and decide....Clear rules should determine the conditions of creation, use, and control of files pertaining to individuals."

PART FOUR: POLICY ANALYSIS AND RECOMMENDATIONS

Our study has shown that personal medical records are being used in an enormous variety of settings -- in every aspect of primary care, for service payment and quality care review, and in all the evaluative Zone 3 activities including employment, credit, licensing, law enforcement, social research and political life. Given this diversity, no single piece of legislation, or judicial rule, or systems guide, or managers' code could encompass all the important problems that require formulation of policy, regulation or supervision. Thus, our initial assumption is that the consistent national approach we seek must be evolved through a mosaic of policies, applied by different authorities and institutions in our society.

A second basic assumption is that guarantees of individual rights must be an integral part of any system of health care regardless of how our national health system develops or how computerization is employed to assist that development. While there is growing public recognition of the centrality of individual rights to computerized health data systems, our study revealed that these systems are evolving on an ad hoc basis, with ill-defined goals and imprecise standards. That is why it is important now -- at the threshold of both fundamental reorganization of health care and of vastly expanded and more sophisticated computerization of personal health data -- to formulate coherent policy that gives due weight to both the rights of individuals and the social and medical needs that computerization serves. The discussion that follows will consider basic policy concepts: how to apply them; how to regulate and supervise them; and what voluntary and professional groups can do to achieve their acceptance.

GENERAL CONCEPTS GOVERNING DATA SYSTEMS IN A DEMOCRATIC SOCIETY

The decade-long public debate on privacy and data banks has seen the emergence of some generally accepted concepts. Briefly, these are:

1. The Contract Theory of Informational Privacy

The traditional civil liberties formulation of informational privacy is that an individual has the right to determine, in most circumstances, what information about him/her is obtained and used by others. But where data systems are involved, there is growing recognition of what might be called an exchange theory -- that the individual releases valuable personal data either in order to obtain a specific benefit or to fulfill a legal duty. In exchange, the data user has two obligations: to use this personal information only for the purpose authorized, and not to treat it so carelessly or maliciously that it harms the individual from whom it was obtained. This exchange or "contract" theory recognizes that personal information -- age, income, race, health conditions, etc. -- has become the vital raw material of business, government and political decision-making, and withholding it would have serious adverse social consequences. Making informational privacy a property as well as a human right is useful in a capitalist society: it buttresses the individual's claim to exert control over the uses made of his/her valuable property. It also underscores the need for a reciprocal duty on the part of the data user to adhere to the informational contract.

2. The Special Dangers of Automated Data Systems

Despite impressive advances, computerization is not yet a completely stable and disciplined technology. We must take it for granted that automated systems have a propensity to go awry, producing the mistakes and "bugs" that have become a well-known feature of computerized operations. This is not to say that computers should not be used, or that harm must be taken as inevitable. But where risks to citizen rights are involved, this calls for special attention in the planning process and continued close monitoring.

3. Responsibilities of the "Data Keeper"

It has become clear that the organization that owns a data system is responsible for its ethical use, and that this responsibility cannot be transferred to others participating in the system -- data processers, contributors of data, regulatory

agencies, etc. The obligations of the data keeper are not only to the individuals whose data is contained in the system, but to society as a whole because the operations of each individual data system affect the general public and contribute to societal norms of organizational responsibility. Because of these larger societal concerns, general standards are evolving to measure the performance of data-keepers. These standards are gradually being translated into law as statutes or regulatory agency rules. Among these standards are:

a) Only information relevant to the organization's legitimate purposes should be collected and stored. "Relevance" is limited by constitutional guarantees of privacy and prohibitions against discriminatory use on grounds of race, sex, cultural differences, etc.

b) The data collected must be accurate, timely and complete.

c) Disclosure of personal data inside the organization should be on a strict "need-to-know" basis.

d) Disclosure of personal data outside the organization should be made only with the informed, voluntary consent of the individual, and not dependent upon implied, "blanket," or general consent.

e) An individual should have the right to see his/her record and to consent to the accuracy, timeliness and pertinency of its contents. While there may be a few justified exceptions to this rule, they should never be invoked if the record is used to make judgments affecting the individual's rights and benefits.

4. Requirement of Public Notice and Review

The creation of personal information data systems is too important to treat as an internal management prerogative. There should be widespread advance public notice of plans to create or expand data systems so that citizens may understand their purposes and examine the citizen rights safeguards. An already operating personal data system ought to be subject to continuing evaluation by outside, independent bodies, with mechanisms for redressing legitimate individual complaints.

TWELVE BASIC PRINCIPLES FOR HEALTH DATA SYSTEMS

Having identified these concepts, how can they be applied on a practical, day-to-day basis to health data systems? The traditions of the medical profession impose some unique burdens on building citizen rights into health data systems, chief among them that physicians believe they must protect the mysteries of the medical profession from common view and that they alone must decide what patients should be told about their conditions. The tradition of doctor-patient confidentiality is a positive, countervailing force, but it is often swept aside in practice and by the law as to circulation of patient information.

The following principles attempt to take these medical traditions into account, and to draw upon experiences of organizations presently applying them in an exemplary way.

1. Requiring Public Notice and Impact Statements

> Principle. Plans for automated data systems using identified personal medical records should require advance notice filed with an appropriate outside authority and communicated to individuals whose records will be affected. This notice should include a "privacy impact" statement describing how the proposed system would affect the organization's existing citizen rights practices.
>
> Among the basic elements of the notice should be: purposes; type of information to be collected and stored; uses to be made of the data; rules for confidentiality and access within the organization; rules for releasing identified information to outsiders; provisions for patient access and review; provisions for assuring accuracy and timeliness of data and for purging stale data; provisions for physical security of data.

For federal agencies in the health-care field, a requirement that all personal data systems be disclosed and that rules governing them be published in the Federal Register are basic requirements of the Federal Privacy Act of 1974. Similar notice requirements are in five state fair information practices laws. However, no privacy impact statement is required by these laws, and there is no regulatory body that has authority to receive and act upon what the agencies disclose.

Since primary care for most Americans is being delivered today in local and state hospitals and private institutions not covered by these laws, the need to mandate a system for such notices and impact-statements is still very much with us. There are at least three main approaches to such action:

A. For private institutions, let notices and impact-statements be filed with a private commission, representing both professional and public-interest groups, and let it deny accreditation as an ethical data center to any institution that fails to meet defined standards and safeguards.

B. For state and local health agencies, look to state law to create either the public-notice system required by fair information practices laws or a system that vests supervisory power in a state commission, along the lines of the Swedish Data Protection Board. The latter system might also extend state regulation over all private health data systems, in recognition of the state's historic responsibility over health matters as well as citizen rights.

C. Expand federal regulations into this area, as by instituting a system of notices and impact-statements that is national in scope, like securities registrations under the Securities and Exchange Commission. A less sweeping approach would be to create a special health-data system commission at the federal level that would pass upon data system notices and impact-statements on the theory that the sensitivity of the data here required a coordinating and supervisory mechanism beyond the Federal Privacy Act.

The pros and cons of these different approaches -- in terms of government versus private responsibility, state versus federal jurisdiction, and regulatory-agency versus judicially-enforced standards -- are explored in the main report. Whichever techniques may be adopted through public discussion and experimentation, the principle of notice and impact-statement is critical if we are to insure a level of public decision-making for an area that is too important to continue as a matter of ad hoc managerial policies.

2. Setting Limits on the Collection and Recording of Personal Health Data

> Principle. An organization creating a health data system should examine whether the collection and/or recording of each element of personal health information is essential for carrying out the organization's proper functions. Socially acceptable standards of relevance and propriety should be worked out for data systems through public discussion and policy-setting mechanisms.

Zone 1. Within the primary care zone, it is generally accepted that extensive disclosure by the patient is needed for effective diagnosis and care, and therefore, all data volunteered by the patient is essential, relevant and proper. If the relationship were limited to doctor and patient, no privacy questions would arise out of such extensive disclosure. But within the primary health care zone, many individuals not directly connected with the patient's care have access to the patient's record. More important, the flow of medical information from Zone 1 to Zones 2 and 3 is seldom accompanied by guarantees of its confidentiality in wider use, protections against its adverse use in evaluative decisions, by the informed consent of the patient to its dissemination, or by the opportunity for the patient to correct harmful inaccuracies. Without these safeguards, the claims of primary care facilities to record such extensive, sensitive information must be evaluated in terms of their likely uses and exposures beyond the primary care facility.

Zone 2. In the recent past, the underwriting/eligibility process allowed health insurers wide discretion in rejecting applicants on the basis of arbitrary criteria -- race, sex, homosexuality, "morals," etc. During the past decade, however, the law and regulatory agencies have moved to limit the imposition of such criteria. Race, as an overt criterion for health insurance is forbidden. Different benefits for males and females within the same occupational group or other classification has been attacked before regulatory bodies and in the courts, and the health insurance industry

has recently adopted a policy against such discrimination, as well as agreeing that homosexuality per se would not be used as a basis for rejecting an applicant.

Many of these exclusionary policies were unrelated to the actuarial realities, but even where certain eligibility decisions could be shown to be "relevant," our changing perceptions of citizen rights might prohibit their application because they are inappropriate in a pluralistic society. In such cases, we should recognize that we are socializing certain risks, accepting the idea that all policy-holders will have to share the cost of not allowing companies to exclude persons whose conditions may, in fact, lead to higher costs because of increased morbidity or earlier mortality. That is one way society can prevent continued harm to persons whose "objective" situation is the product of past discrimination. Whether accomplished through industry self-regulation, state insurance regulation, amendments to the Fair Credit Reporting Act or new legislation, new standards of relevance and propriety in the health underwriting process should be a major effort. These new standards will be effective only if underwriting practices -- application forms, investigative reports, etc. -- are carefully scrutinized to screen out the collection of irrelevant or inappropriate data, and the uses of properly collected data are monitored.

When we turn to the claims process, we must recognize that identification of the individual, description of the services provided, diagnosis and similar key information are essential to payment of benefits. Such information is also needed to control fraudulent practices by health providers and institutions, and to supply a data base for future rates, coverages and programs. However, the legitimacy of the service payer function has often been used as an excuse for collecting and keeping more personal information than the claims function requires. Our study found that lack of trust in the confidentiality practices of claims payers was widespread among professional groups.

This problem does not originate with service payers alone. Some hospitals send a whole medical record rather than take the time to extract the specific information requested. Some psychiatrists use vague terminology deliberately to secure reimbursements not covered in a policy, leading to demands for more detailed information. In response to these professional-service payer tensions, both groups are seeking to tighten their claims review processes -- to limit requests for data to only those needed (Blue Shield); to urge hospitals to require insurance companies to specify why they need certain information; to return the record within a specified time or to destroy it on completion of the claims review (medical record administrators); to deny employers holding group policies access to sensitive employee data from insurance companies (agreement between the Union of American Physicians and Aetna Life and Casualty Company).

The key issue in quality care review is the removal of personal identifiers from the records reviewed. This will be critical in securing public support for any proposed universal health insurance plan where the problem of a federal medical record system raises special, post-Watergate sensitivities. As the PAS system demonstrates, there are ways of stripping personal identifiers from each record, and given their proven practicality, the burden of proof should be on each quality care review system (and in each exceptional individual situation) to show that it cannot operate without unique identifiers; absent such a showing, it should be the duty of care reviewers to devise a system that does not use or store identified personal records.

Zone 3. Our society accepts the lifting of medical confidentiality in cases where some clear social benefit accrues from the dissemination of personal health data -- recording births and deaths, reporting of communicable diseases, etc. But there is a large area of such dissemination in Zone 3 where the social benefit is less discernible and where the harm to the individual may be serious and permanent. It is in these areas that the production of personal health data for non-medical uses is being re-examined. Among the questions being raised are how relevant past health conditions are for present judgments, and whether certain medical conditions -- past or present -- should play a role in decisions on employment, licensing, credit, government benefits, etc.

The employment area is a good one to illustrate the application of the relevancy principle. At one end of the spectrum is the requirement of medical data that is clearly job-related -- food handlers must be free of communicable diseases; airline pilots should not be subject to blackouts. At the other are those employment application forms which demand histories of past conditions (e.g. bedwetting), about past and present emotional problems, including whether the individual is presently receiving psychological help. A study by two Veterans Administration doctors

documented that industrial physicians would recommend against hiring persons with mild illnesses, and that the criteria used "have little relation to modern medical judgment."

Some companies have altered their pre-employment health questionnaires to take account of citizen rights. IBM, for example, conducted a privacy review during 1974-75, and discovered that questions about past emotional difficulties caused resentment and sometimes evoked untruthful answers. Moreover IBM discovered that there was no medical or social evidence that persons receiving professional help for emotional problems were worse employment risks than those who were not. As a result, IBM dropped questions about emotional disturbance from its pre-employment questionnaire. The company has also developed privacy standards for those already hired. When employees are given physical examinations by IBM or private physicians, the results are kept confidential, and IBM managers are not told the specific health reasons when work restrictions are set by the company medical department. An employee's health condition is never included in IBM's automated personnel data system.

3. Notifying Individuals of Data Policies when their Information is Sought

> Principle. When an individual is asked to supply personal information to be included in a health data system, he/she should be given a clearly-written account of how that information will be used by the collecting organization, and what procedures for obtaining consent will be followed before any additional uses will be made within the collecting organization or identified information is supplied to other parties.

The Federal Privacy Act and its state counterparts require that individuals be informed at the time the information is sought of how their data will be used and what the organization's rules for data sharing are. Our project's initial impression is that compliance with this new law has been good. The one complaint we heard involves fears that an organization might want personal information for some later purpose that would not have been described and consented to at the time of the original collection. For example, health professionals feel that asking patients for consent to use their later data -- as for follow-up research in drugs thought to cause cancer which appears many years later -- might alarm patients unnecessarily before the possible effects have been confirmed.

Rather than abandon the principle of describing present and future uses at the time of collection, the explanations developed by health facilities should be drawn up with such possible contingencies in mind. If some unforeseen development occurs, either subsequent consent could be obtained, or the additional use might be authorized by some independent review body. Whatever technique may be adopted, hypothetical future possibilities should not be allowed to undermine the requirement of notice.

4. Information Release Forms Should be for Specific and Limited Purposes

> Principle. General release forms do not meet proper standards of citizen rights. The forms used to release personal information from a health data system should be for a specific purpose, should describe the information to be released, and be limited in time for which the release applies. Adequate procedures must be followed to obtain the individual's voluntary and informed consent to any release. Provision of entire medical records should be permitted only upon use of a special release form, reviewed by a special officer of the record-keeping organization. Organizations seeking release of information must file with the record custodian a form indicating how they would use the data, specifying that it will not be released to other parties without the individual's consent, and indicating what their information retention or destruction policies are.

The general release in the health field recalls the general search and seizure warrants used by the British in Colonial America -- the "fishing expeditions" now prohibited by the Fourth Amendment. While law enforcement and health care are very different, the analogies in civil liberties terms are, alas, all too close.

Individuals are being asked today to sign releases that allow institutions to disseminate personal medical information however, and to whomever, the institution wishes, or that allow someone offering a benefit or service to the patient to

examine "any and all" medical records in any doctor's office or health institution. In no sense is this informed consent: patients do not know what is in their records, or what segments of it will be opened to third party access, or what will happen to the information once it is in the third party's hands.

Such practices, bad as they were in the manual-records era, cannot be permitted to persist in large-scale health data systems, with increasingly comprehensive records being generated and preserved in primary health care facilities. A few health centers and hospitals recognize the inherent disadvantage that general release forms impose on patients and have substituted specific forms. Our profile of the Martin Luther King, Jr., Center, for example, described its requirement of informed, voluntary patient consent to the release of information. But MLK and other neighborhood health centers are not as highly automated as the large health data systems, and it is there that more detailed and protective policies are especially needed. These policies should include all of the items listed in the above Principle, with special emphasis on explaining to the patient what will occur if the information is supplied -- or not supplied -- so that he/she can decide whether to reveal or withhold it. Release forms should be revocable by the individual within a specified time, and this right should be fully explained, including the potential harmful consequence to the individual of such revocation.

5. Increasing Patients' Access to their own Medical Information

> Principle. Individuals should have a general right to information about their health condition, treatment and prognosis as part of the professional's fiduciary duty and as protection of the patient's primacy in choosing his/her health destiny. In health data systems, the individual should have an absolute right to inspect any recorded data about him/her used to make judgments about eligibility for health programs, claims payment and other aspects of service administration. Absolute right of access should also be provided when health data are disseminated to determine non-medical benefits or opportunities. Where necessary, medical terminology should be explained, and individuals permitted to challenge the accuracy or completeness of recorded data.
>
> Where parts of the medical record contain the health professional's working notes or other informal materials, or sensitive judgments about emotional conditions that might unduly upset the patient, and these materials are used solely within the primary care facility, a three-step process in either chronic or acute care situations should be instituted. First, the health professional should discuss directly with the patient why such access might be unwise. Second, the health professional should recommend that disclosure be made to another physician of the patient's choice, who could then evaluate it and disclose it if he/she felt it was in the patient's best interest. Finally, if the patient rejects both these options, the patient should have the right to see the record, with whatever explanations of terminology the health professional feels important to give.
>
> In the case of psychiatry, where institutional care is involved, the same multi-stage process should be used, except that the third stage should be a procéeding by which the individual or his/her legal guardian applies to a civil court, which decides after a hearing whether or not direct disclosure should be made. Where individual psychiatric care is involved, the procedure should be the same as with chronic or acute care, except if the psychiatrist believes withholding the record is so important to the patient's well-being that the psychiatrist is willing to end the therapist-patient relationship. In that case, the record need not be revealed at that point; however, any patient who still wished to secure it should have the right to apply to a court and maintain the same proceeding described above for institutional care.

The question of patient access is controversial and complex -- controversial because it involves deeply-held perceptions of how doctors and patients view themselves and their relationship; complex because it involves scores of possibilities that call for finely-tuned judgments difficult to encompass in a universal principle.

The traditional view of most health professionals is that the ethical physician has the duty to decide what information it is in the patient's best interests to know. Withholding information may be good medicine in some cases; disclosing it may be good medicine in others. But in any case, only the physician can make this decision.

The more recent view rests on a "consumer" theory of health care. It sees the physician as an agent of the patient, hired to exercise professional skills and to make full disclosure to the patient whenever it is requested. Such a right to full disclosure is essential to the patient in making informed decisions about the risks and benefits of proposed treatments and operations and making comparative judgments about the adequacy of care provided by doctors and hospitals. While some patients may be so emotionally distraught that they cannot handle full information, those adult patients who ask for it should not be denied it, including information about terminal illness, where a patient wants to decide how to use the remainder of his or her life.

When the issue of disclosure shifts to access to medical records (as distinguished from medical information), the consumer position argues that since the records are seen by a variety of health providers, it is essential that a patient who feels that erroneous data has gotten into the record be able to correct it before erroneous care decisions are made. Moreover, examining the record is the only way patients can decide whether to release some or all of it for third party use. Providing access would also decrease the number of malpractice suits filed by patients who are doing so today because that is the only way they can get to see their records. Finally, the consumer position believes providing access would enhance confidence in care and cooperation in treatment.

The traditional medical view counters that the technical terms in medical records would confuse the patient, and explaining these terms is time-consuming and expensive; patient access would inhibit speculative and hypothetical entries which help both the physician and professional consultants; it would lead to defensive record keeping practices; and it would make medical records less valuable for service payment, medical research, care-review and other uses.

The law has done little to resolve this controversy. As to patient access to information, courts have held that a doctor must inform the patient of the risks and potential outcomes of any dangerous procedures; on the other hand, in ordinary care, courts have upheld a doctor's right to decide what information to disclose or withhold in the patient's best interests. As to patients' access to the record, in the great majority of states there is no statute or case law declaration of the right of patient access to doctor or hospital records, and only when a patient files a lawsuit is he entitled to a copy of his/her entire record.

It should be noted that computerization accentuates the problems on both sides. For patient-consumers, the richer, more complete, more permanent and more easily disseminated material in automated records heightens concern about what is in them. For doctors, computerization of detailed progress notes, informal diagnoses, and observations on emotional and social conditions heightens concern that these printouts will be secured by patients and shared with their lawyers and friends. At the same time, compared with manual records, a computer system makes it easier to print only selective portions of the record and to suppress securely all parts of it that are not to be given to a particular inquirer -- patient, insurance company, researcher, policeman, etc.

Although recognizing the validity of some of the concerns raised by the traditional medical view, our recommendations move toward increasing rights of patients access. This is for two key reasons. First, American health care is no longer the one-to-one, family doctor model. Factors such as our high population mobility, group medical practices, increasing medical specialization, treatment in hospitals and neighborhood health centers rather than at home -- all these and other factors dictate that most patients will be treated by scores of health professionals. Thus, it makes little sense to install a national legal rule of patient access geared to a treatment setting of sustained, single personal relationships that exists only for a small minority. Second, we are entering a period of change in the format and content of medical records, spurred not only by professional dissatisfaction with present inadequacies, but by pressures to meet increasingly strict payment and care review requirements. This condition of change being the case -- and with the information-handling capabilities of the computer to draw upon for innovative solutions -- we ought not to allow the present character of medical records to dictate what would be the best access policy for the future, especially

for automated health data systems.

For these reasons, we suggest a "dual" system of medical records. The first part, which would be the official record, would consist of all the personal data about the patient -- personal history, tests, examination results, treatment summaries, payment data, etc. The patient would have a full right of access to this part of the record, with a procedure to explain medical terminology.

The second part would consist of any especially sensitive judgments, or speculative and tentative hypothesis. Such materials would not be available for any other uses beyond primary care. The procedures for patient access already set forth in the above Principle as to sensitive conditions and working notes apply to the second part of the dual record we propose. It would also be reachable through subpoena by the patient in a malpractice case, just as physicians' notes are now, and obviously, as now, anything a physician did not think it safe or wise to write down would not become part of any record.

While the dual record system and patient access concept have been gaining support among public interest groups, and from some in the medical community, it has not yet won widespread acceptance among doctors or health administrators. That acceptance might be achieved over a period of years through the examples of its successful application and through professional debates and advocacy. But the major expansion of health data systems, the development of regional systems, and the prospect of national health insurance all suggest the need for a less leisurely approach. When such major steps are taken, we believe the line has been crossed at which intervention of law ought to take place, at least for the records in those health data systems.

6. The Duty to Insure Appropriate Accuracy

> Principle. The managers of a health data system must see that the personal data they store are as accurate, timely and complete as their uses require, not only to assure proper health care but to protect the opportunities and benefits of individuals that may be determined through use of such data. Review by the individual of his/her records before release to third parties, and affording individuals a general right to access, represent helpful ways to improve accuracy in such data systems.

Whether or not patient access is afforded, managers of health data systems have the duty to see that the records are accurate. The standards for a given area will depend on how the records are used. In primary care, for instance, reliance on the result of an outdated lab test for medical decisions would be unacceptable, as would relying on a school nurse's comment that a child's fit "looked like" epilepsy. The more comprehensive a health data system, and the more its records are relied on, the greater the attention that must be paid to accuracy.

7. The Duty to Apply Appropriate Data Security Measures

> Principle. Because of the sensitivity of personal information stored in a health data system, security measures must be taken to limit access by personnel within the organization on a need-to-know basis, to monitor data uses to detect unauthorized conduct, and to protect files against outside penetration.

This is one of the least controversial principles for health data system managers, and there are well understood techniques that computer experts apply to insure the necessary level of security for a given data system. The key issues that arise are: (a) the need to formulate clear policies as to data access; (b) the need to assess foreseeable threats to data security based on prior breaches in the manual-record era and any new risks posed by especially attractive records; (c) the need to adopt a variety of physical security measures (locks, passwords, audit trails, etc.): and (d) the need for special measures to guard unusually sensitive files such as psychiatric records in a general hospital, as by storing them on separate minicomputers in locked facilities.

8. The Duty to Inculcate Respect for Citizen Rights

> Principle. Every health data system should develop intensive orientation programs to foster understanding and acceptance of both the spirit and the letter of the system's policies on citizen rights by the organization's own personnel. Such programs should recognize and deal with the special attitudes of major occupational groups in the organization (doctors, nurses, administrators, data processers, etc.). Where possible, patients and public representatives should be included in the development, management and evaluation of these educational programs.

Any important organizational changes, such as the principles proposed here, are bound to encounter some hostility from those accustomed to the "old" way of doing things. Formal notification to employees of new policies is an important first step in assuring compliance, but by itself cannot overcome the inevitable resistance. Far more important are the positive attitudes of top management in promoting understanding of citizen rights through orientation programs, continuing seminars, problem-solving sessions, special training materials, etc. The success of the Martin Luther King, Jr. Center, IBM, and Drs. Weed and Golodetz in promulgating confidentiality and patient access standards are examples of the planning, communications and evaluation efforts that must go into achieving staff acceptance of innovative policies in an on-going organization.

9. The Need for a Patient's Rights Handbook and a Patient's Rights Representative

> Principle. Every health data system in primary care should publish a clearly written handbook on patient's rights and responsibilities that is given to each individual at the earliest point of contact with the facility. Each system should also have a patient's rights representative or ombudsman whose availability and duties are described in the handbook. While a rights handbook and patient representative should not be limited to record-keeping and data issues, the creation of a data system is a key opportunity for organizations without such services to create them.

The experience at the Martin Luther King, Jr., Center shows that the very publication of a patient's rights handbook helps orient the staff to its responsibilities, improves patient-staff relationships, and serves as an objective guide for the resolution of citizen rights disputes. The critical element in making patient's rights more than a paper declaration, however, is the day-to-day presence of an independent patient's rights representative to whom patients can complain or seek help and who will serve as their advocate in disputes with the staff and administration.

10. The Need for Independent Audit and Periodic Review

> Principle. Because EDP use is a continuous process of expanding initial computer applications to additional files, creating new combinations of data, and extending data utilization, any health data system must be subject to regular review by an independent body. Such periodic review should focus not only on the continuing adequacy of the organization's policies and data security, but also examine any major expansion of the data system that would have significant impact on citizen rights.

If projects to develop integrated hospital information systems, lifetime patient medical histories, regional planning systems, etc., progress as their proponents predict they will, the next decade will be a time of rapid change in health care computer use. Thus good public policy requires that outside review of an organization's data system not be treated as a one-time certification process, but recognize the essential dynamism in health computerization. The same mechanism suggested for reviewing the creation of health data systems should be explored for conducting continuing reviews.

11. The Need to Insure Information for Public Oversight

> Principle. There is an inevitable tension between the individual's right of privacy and the public's right to examine and supervise how its social institutions are operating. The confidentiality rules established by health data systems should be examined to avoid adding to existing difficulties in policing compliance with health program requirements and assessing the quality of health care. Using medical records without unique identifiers, or with potentially identifiable data removed, is the major technique for softening the conflict between privacy and public access interests.

We have already touched on removing identifiers from medical records used for quality care assurance. Its importance is underscored by the fact that the public authorities charged with policing fraud and assuring quality care are often part of the same governmental branches whose violations of privacy, confidentiality and due process have shocked the public in the past few years. What is needed to restore public confidence is the enactment of statutes or regulations that are clear as to the uses that can be made of data obtained for public oversight, with workable prohibitions and penalties against misuse. There is also an important need to provide such access for public interest groups, the media and other participants in the process of public criticism and review.

12. The Importance of Research and Evaluation Using Health Data

> Principle. While securing informed, voluntary consent should cover most situations in which identified data is used in medical research, there will be times when this is not possible. In these cases, the health data system should have the purpose, procedures and safeguards of the research reviewed by a special panel of representatives of the data system, independent scholars of high reputation, and public interest groups relevant to the research project (minorities, women's, civil liberties groups, etc.). Securing legal privilege against compulsory disclosure of research records should generally be a prerequisite for a health data system's agreement to participate in a research study, disease register, or program evaluation involving sensitive personal information.

We noted that in the past there had sometimes been a cavalier attitude on the part of researchers towards their subjects -- conducting "voluntary" experiments on prisoners, on patients not told that they were subjects; on patients denied treatment so that the course of a disease could be studied, etc. While these abuses did not involve record-keeping violations, their revelation fanned public hostility to the creation of state computerized health data systems for research or evaluation purposes. The failure of many such systems to create detailed safeguards against misuse of research data further undermined confidence in them.

Obviously medical research must continue to seek the answers to pressing health problems, and identified medical records are needed for this research. And equally obviously, program evaluation to help us select the best method for delivery of medical care at the lowest cost must go forward, and this, too, sometimes requires examination of identified medical records. Past practices in the research and evaluation field have led too many people to conclude that the goal of protecting citizen rights is incompatible with the goals of research and evaluation. It is not. It will take conscientious efforts to secure informed voluntary consent from patients, or where that is not possible, to create the review panels suggested, and in either case, to secure legal privilege against compulsory disclosure to third parties. These steps will not only insure citizen rights, but ultimately they will also strengthen public acceptance of needed research and evaluation.

CURRENT PRIORITIES FOR POLICY ACTION

The work of refining and applying these twelve principles for health data systems is clearly a long-term task of public policy. From our investigation of emerging citizen rights problems in the health field, we can identify an agenda of issues that now seem ripe for action. We will mention examples of issues that require action through legislative, judicial, organizational, and citizen-group initiatives, to stress our conviction that such a mixture of interventions is vital to intelligent policy in the coming years.

1. Legislative Priorities

Some legislative actions involve pin-pointed reforms, in the recognition that society does not think it wise to let these matters be worked out slowly (and uncertainly) through judicial decisions or the fair information practices law route. For example, Congress ought to bring the use of medical information in credit, employment, and insurance reports under the protections of the Fair Credit Reporting Act. One can understand why the legislators in 1970 decided not to include such data when they took their first major step to regulate commercial reporting services, but the record of the past five years has made it plain that consumers deserve to have access rights when medical data is used to deny them credit, insurance, and employment. There are important issues to work out in such an amendment to the 1970 Act, such as whether the individual would see such information directly or have a physician of his choice receive it. But the need to remove the medical exemption from this consumer-protection law flows directly from the principles presented earlier, and nothing presented by industry spokesmen at hearings on this issue is persuasive to the contrary.

Enactment of medical-research laws at the federal and state levels is another specific legislative action that deserves priority treatment. We have already discussed the absence of such legal privilege today and the continual pressures on such data from law enforcement officials, administrators, and other government bodies. A carefully drafted medical-privilege statute ought to command wide professional and public support.

Given the confused and uneven laws in the 50 states on confidentiality of medical information and patient access to records, the development of a model statute and its enactment by as many states as possible would be an important step toward modernizing citizen rights in this area. The American Medical Association has been working on the draft of such a model statute for several years, and their latest version is a thoughtfull approach that has merit. While there will be important differences between the AMA and other groups on some aspects of this law, the AMA model bill represents an excellent starting point for discussion. If civil liberties and public interest groups could work cooperatively with the medical profession on refining this measure, and agree to disagree where that is called for, this coalition could provide the driving force for state legislative action. Similar coalitions between civil liberties groups and bankers associations have been important in fighting for privacy of bank records, and a coalition between civil liberties groups and labor unions produced the state laws enacted recently to control compulsory use of polygraphs by employers for hiring and other employment decisions.

With only 5 states having enacted fair information practices laws, anyone concerned with the protection of citizen rights in state, county, and municipal health facilities ought to be pressing their states to join Minnesota, Massachusetts, Utah, Arizona, and New Hampshire in placing government data uses under protective legislation. Indeed, as the Privacy Protection Study Commission holds its hearings in 1976 into the administration of the federal and state privacy acts, and writes its report on the successes and problems that have surfaced thus far with such laws, a stronger and improved model of the fair information practices law may be developed for other states to adopt.

Finally, explicit citizen rights provisions and a general administrative system that facilitates such rights should be installed in any national health insurance program enacted by Congress. The confidentiality and individual-access policies just enunciated by HEW to govern professional standards review (PSRO) for Medicare and Medicaid are excellent standards, and while there is no experience yet as to how well they will work, these policies could be drawn upon for national health insurance bills and regulations. Many of the principles are already in these PSRO policies and could probably be adopted for national health insurance without too much struggle. However, several areas of sharp controversy can be predicted.

While some will see national health records as valuable sources for other social purposes, protection of citizen rights requires that the law have provisions declaring that national health insurance data can be used only for administration and evaluation of the insurance program, and that identified records will not be accessible for any other governmental or private purpose (such as location of deserting fathers, income tax enforcement, police investigations, private lawsuits, etc.).

Some legislators will want to follow the easy path of using the Social Security number for this system, but use of a unique national health insurance number would protect citizen rights by not having medical records include a number that is often known to others and whose presence in these records would facilitate their linkage with other files.

The tendency of many experts designing the administration and data systems of a national health insurance program will be to have summaries of identified records for every participant held in one file in Washington, as Social Security records are now held. They will also want to have patient-identified records of cases on appeal for denial of payment or provider fraud also sent up to regional offices and to Washington. Here too, proper concern for protection of citizen rights should lead to a rejection of such approaches in favor of a system that has identified records kept only at the local level, with the local agency generating a special, randomized review number and removing all unnecessary personal information from any record sent up for review to regional or national offices. Since the provider's identity would be preserved in all records, this ought not to interfere with the audit trails necessary to police against suspected fraud or misconduct.

Finally, some legislators will want to use the "doctor-knows-best" principle to govern an individual's access to his/her record in the national health insurance system. Following the principle already presented in this section, we believe that if a medical professional has not been able to convince a patient through personal counseling that direct patient access is unnecessary or unwise, then refusing such access cannot be in the best interests of the patient or consistent with the professional obligation of the physician, and access should be permitted by law.

2. Judicial Actions

Test cases are the accepted way that individuals and groups seek to activate the American state and federal judiciary to advance citizen rights. But beyond such specific lawsuits, we think there is a broad strategy that ought to be directed at the courts in the coming years, to establish the common law duty of private organizations and the constitutional duty of government organizations to take reasonable care in the way they handle sensitive personal health data. Where this is set by statute or regulatory order, of course, that would define such a duty and make it enforceable at law. But even in the absence of such laws, we think that there is a failure of legal duty whenever a health data organization does not adopt (a) explicit policies to assure rights of privacy, confidentiality, and individual access; (b) procedures to assure appropriate levels of accuracy, timeliness, and completeness; and (c) adequate data security measures to control improper uses. What constitutes sufficiently explicit policies, appropriate accuracy, or adequate security measures would be defined according to the type of organization and activity involved, and the existing state of the art in data security equipment and techniques. Lawsuits could be brought either by individuals whose interests in privacy and medical care were threatened by organizations using their data without meeting such standards, or by public-interest groups sponsoring class-action suits in the same vein.

It can be argued that setting such standards should be the work of legislation, executive order, or regulatory-agency action, and that invoking the courts is neither responsible public-policy for a democratic society nor a good way to hammer out the detailed rules so often needed. It could also be argued that this would not give organizational managers and computer-systems developers the advance rules they need to avoid ambiguity, and to help justify committing money and staff to the task. Yet the genius of the American judicial system has been its development of new duties for private parties (and redefinition of constitutional rights) to reflect new business activities and technological change. In the common law, this was the way new concepts of contract were developed for mercantile capitalism, and new concepts or tort law for industrialization. Judges today could be equally creative in defining the legal duties of those who use information technology. A failure of duty would be careless and negligent treatment of sensitive personal data, and successful practices would show what is reasonable (and practical) to conduct. After several leading cases had set the main lines of acceptable and unacceptable conduct, the organizational managers and

systems developers would have the guidance they sought, and society would have activated an important way of achieving continuing review of organizational responsibility.

3. Organizational Responsibilities

Legislation and judicial decisions take time, and it would be unrealistic to think that many of the priorities just discussed will be installed immediately. This leaves the immediate initiative for action with organizational managers. Furthermore, the standards that will be used by legislators and judges are often drawn from good as well as bad organizational practice in the industry or programs being regulated. This means that the interests of organizational managers in avoiding unwise regulation as well as in the discharge of their own leadership responsibilities makes it important for managements to address such citizen rights issues themselves.

We think any organization maintaining a large-scale data system ought to conduct the kind of serious, in-house "privacy audit" of its principles, policies, practices, and procedures that IBM did in 1974-75; that most federal agencies did in 1975-76 in preparation for complying with the Federal Privacy Act; and that many businesses have been doing in 1976 to see that they are not engaging in controversial practices that would support the enactment of proposed federal measures such as the Koch-Goldwater Bill, H.R. 1984. Such a privacy audit should surface the real problems in the organization; its prime advantage is that it then allows managements--with whatever outside help they may need--to deal with those issues directly and carefully, rather than having the problems accumulate and worsen through management inattention, unfocused data-system decisions, and similar developments.

At the same time, many professional groups have been working recently to formulate new sets of guidelines to deal with citizen rights issues in the health field. These include new guidelines from Blue Shield, the American Society of Internal Medicine, the American Psychiatric Association, community health centers, social workers, nursing home operators, and many others. The concept of creating and legalizing "ethical data centers" that Dr. Elmer Gabrieli and his colleagues have advocated offers another valuable source of guidelines to draw on. The enunciation of such guidelines has played an important role in American society in defining good practice and professional standards, and it deserves to be used to the fullest in extending citizen rights in the health fields.

4. Citizen Group Actions

Beyond health-professional organizations, our study has shown that the American Civil Liberties Union has played the single most important role in raising citizen rights issues during the past few years. This has been not only through the activities of the ACLU National Office and its state affiliate chapters, but also through various projects directed or supported by the ACLU, such as the Mental Health Law Project, the Prisoners' Rights Project, the Juvenile Rights Project, and the Project on Privacy and Data Collection. One does not have to agree always with the position taken by an ACLU chapter or the national office to recognize that the continued attention--indeed, the increased attention--of ACLU to health-data issues is going to be essential to the working out of good policy in the coming years.

Beyond that, the recent formation of the National Commission on Confidentiality of and Access to Health Care Records is a promising development. Composed of 18 leading organizations in the health field, and growing out of the excellent conference on confidentiality held in Key Biscayne, Florida in late 1974, the Commission could well sponsor just the kind of activities in research, legislative-drafting, consulting, and public testimony that is needed to give coherence and consensus-forming mechanism to efforts in this area.

Finally, is there any special role to be played by computer professionals in the protection of citizen rights in health care? It can be argued that computer professionals can make their best contribution within the organizations they work for (e.g. hospitals, state health departments, etc.); as private citizens participating in public debates over databank issues; in meetings dealing with medical computing, such as the MEDINFO conventions; or through the general activities of computer groups such as the Association for Computing Machinery, the American Federation of Information Processing Societies, and similar groups. These are all important activities, yet there is an additional one that deserves consideration. When particular government data systems are being considered in local communities or at the state level, whether these are systems in criminal justice, welfare, health, taxation, or other fields, informed computer professionals can do a great deal to help the public interest groups concerned about citizen rights to understand how such proposed systems will work, or

how existing systems are working. The computer professionals can also suggest how protections can be worked out within such systems, what the costs are likely to be, and how such systems could be effectively monitored. In addition, whenever public advisory groups or independent audit groups are set up for such data systems, the addition of a citizen-rights oriented computer professional not employed by the government is usually essential to such a group being able to exercise meaningful oversight.

Sometimes computer professionals volunteer for this work or do so as members of the public-interest or civil liberties groups. But the relative infrequency of this professional participation (not only in the health field but in others as well) suggests that we may need some kind of organizational assistance. If the major computer associations, both nationally and through their local chapters, could publicize the availability of volunteer experts to help citizen groups, or to serve on public advisory committees and oversight committees, or to advise legislative committees needing help in sorting out the issues, this might provide the kind of linking mechanism that does not seem to be in place yet in the thousands of local communities and state capitols where the tens of thousands of personal data systems are being built, expanded, and regulated.

CONCLUSION

As American society redefines and reorganizes its health-care system in the coming decade, it will have to make increased use of computer technology to manage the rivers of data that will be generated. Vital medical research, public-health studies, and environmental controls will also require increased reliance on EDP, just as there will be powerful benefits from EDP for individual health care, in the development of permanent patient histories, emergency treatment communications systems, and similar patient-oriented activities.

If the question is not whether but how such technology will be used in health care, American society has one non-negotiable condition for this process: basic citizen rights cannot be made a casualty of technology-assisted health systems. To do so would be to betray the tradition of Hippocrates, and ultimately to dehumanize health care itself.

It is the custom of Americans to believe that no "lady-or-the-tiger" choice has to be made between science and liberty. For 200 years, in the tradition of Franklin and Jefferson, we have hammered out legal rules that allow each successive wave of invention to realize its potential, but also required each to be brought under the rule of law. Sometimes it took a while for the principles of regulation to become clear, and we have come to realize that the awesome effects of contemporary technology give us less lead time for social learning and regulatory response than we had in earlier eras. But that is the challenge we face, and there are promising signs that our society understands how important it is to develop, soon, the standards by which we can pursue the benefits of both science and liberty in the field of health care.

NBS Monograph 157 ("Computers, Health Records, and Citizen Rights") and its condensation, Special Publication 469 ("Policy Analysis of Citizen Rights Issues in Health Data Systems"), were prepared under contract to the Systems and Software Division of the Institute for Computer Sciences and Technology, NBS. The contract was monitored by John L. Berg and Michael Keplinger. The manuscripts were edited for publication by Zella G. Ruthberg.

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS SP 469	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

A Policy Analysis of Citizen Rights Issues in Health Data Systems
A Condensation of NBS Monograph 157 entitled "Computers, Health Records, and Citizen Rights" by Alan F. Westin

5. Publication Date: January 1977

6. Performing Organization Code

7. AUTHOR(S)
Alan F. Westin and Florence Isbell

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

Department of Public Law and Government
Columbia University
New York, New York 10027

10. Project/Task/Work Unit No. 640.1116

11. Contract/Grant No. 5-35886

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

National Bureau of Standards
Department of Commerce
Washington, D.C. 20234

13. Type of Report & Period Covered: Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 77-600001

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This is a condensation of the report "Computers, Health Records, and Citizen Rights" by Alan F. Westin, NBS Monograph 157, which investigates the impact of computers on citizen rights in the health record keeping area. Under Dr. Alan F. Westin's direction, from July of 1974 to April of 1976, a small interdisciplinary team did the following: (1) examined published literature from medicine and health, law, computing, and social science; (2) conducted interviews with major computer manufacturers, systems developers, health professionals and civil liberties, public interest, consumer, and minority-rights groups; (3) made on-site visits to six representative health-care organizations using computers to handle personal records; (4) corresponded with 70 organizations in the health field; and (5) subjected an initial draft report to review by a conference of experts in September 1975 and subsequently by about 50 outside reviewers. The findings of this investigation were then combined into this four-part report. Part One describes the world of medical data and citizen rights within the framework of three zones--primary health care (by health professionals), service payers and health care reviewers and social uses of health data (such as in employment, life insurance, and welfare); Part Two treats patterns of computerization in health care in each of the above zones; Part Three contains the profiles of the six health-care organizations that were studied in depth; and Part Four analyzes the impact of computerization on personal health records, presents comparisons with six other democratic nations, and states 12 recommended management principles for health care data systems. The full report also contains a 28 page bibliography and 12 appendices with support documents and information.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Citizen rights; computers, confidentiality; data systems; health records; information policy, management principles; medical records; privacy; record-keeping practices; security.

18. AVAILABILITY

[X] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[X] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13.10:469

[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT): UNCLASSIFIED

21. NO. OF PAGES: 48

20. SECURITY CLASS (THIS PAGE): UNCLASSIFIED

22. Price: $1.05

USCOMM-DC 29042-P74

☆U.S. GOVERNMENT PRINTING OFFICE: 1977-240-848/114

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards [1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of the Office of Measurement Services, the Office of Radiation Measurement and the following Center and divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Center for Radiation Research: Nuclear Sciences; Applied Radiation — Laboratory Astrophysics [2] — Cryogenics [2] — Electromagnetics [2] — Time and Frequency [2].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials, the Office of Air and Water Measurement, and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of the following divisions and Centers:

Standards Application and Analysis — Electronic Technology — Center for Consumer Product Technology: Product Systems Analysis; Product Engineering — Center for Building Technology: Structures, Materials, and Life Safety; Building Environment; Technical Evaluation and Application — Center for Fire Research: Fire Science; Fire Safety Engineering.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations — Office of International Standards.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.

[2] Located at Boulder, Colorado 80302.

J.S. DEPARTMENT OF COMMERCE
Vational Bureau of Standards
Vashington, O.C. 20234

)FFICIAL BUSINESS

)enalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

SPECIAL FOURTH-CLASS RATE
BOOK