Designing Protection for Computerized Health Care Information

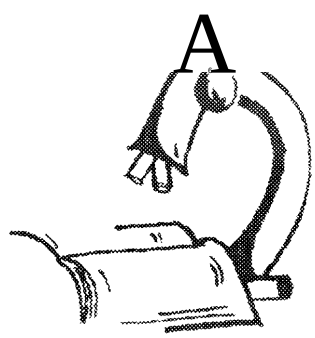
4

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

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

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

- Define the subject matter of the legislation, ''health care information, to encompass the full range of information collected, stored, and transmitted about individuals, not simply the content of the medical record.
- Define the elements that constitute violation of health care information privacy and provide criminal and civil sanctions



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

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

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

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

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

Ethical Tenets for Protection of Confidential Clinical Data

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

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

for improper possession, brokering, disclosure, or sale of health care information with penalties sufficient to deter perpetrators.

Establish requirements for informed consent.

- Establish rules for educating patients about information practices; access to information; amendment, correction, and deletion of information; and creation of databases.
- Establish protocols for access to information by secondary users, and determine their rights and responsibilities in the information they access.
- Structure the law to trace the information flow, incorporating the ability of computer security systems to warn and monitor leaks and improper access to information so that the law can be applied to information at the point of abuse, not just to one "home" institution.
- Establish a committee, commission, or panel to oversee privacy in health care information.

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

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

Uniform Health Care Information Act

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

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

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

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

applicability of their provisions to the needs of health care data protection. This discussion also includes aspects of proposals made by experts in computer privacy issues and certain legislative initiatives.

FAIR INFORMATION PRACTICES AND THE PRIVACY ACT

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

1. There must be no secret personal data record-keeping system.

2. There must be a way for individuals to discover what personal information is recorded and how it is used.
3. There must be a way for individuals to prevent information about them, obtained for one purpose, from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of information about themselves.
5. An organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuses of the data.

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

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

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

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

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

The Act is limited, however, in several significant ways. Some believe that a system of notification through the *Federal Register* is cumbersome

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

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

and burdensome to the individual who, practically speaking, does not regularly review the register, so that notification is not effective. The Act also places the burden of monitoring privacy in information and redressing wrongs entirely with the individual, providing no government oversight mechanism for the system. In addition, the Act itself is limited in its application to ''routine use' of the record, which refers to disclosure of records, not how the collecting agency uses those records internally. Many commentators have noted that the penalties prescribed in the Act are inadequate,[4] and others comment that the Act contains no specific measures that must be in place to protect privacy so that it cannot be used to describe what *technical measures* must be taken to achieve compliance.[5]

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

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

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

FEATURES OF HEALTH CARE PRIVACY LEGISLATION

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

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

[5] Vincent M. Brannigan, "Protecting the Privacy of Patient Information in Clinical Networks: Regulatory Effectiveness Analysis, " *Extended Clinical Consulting by Hospital Computer Networks*, D.F. Parsons, C.N. Fleischer, and R.A. Greene, eds. (New York, NY: Annals of the New York Academy of Sciences, 1992) vol. 670, pp. 190201.

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

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

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

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

The Ethical Tenets for Protection of Confidential Clinical Data ("Ethical Tenets") define the subject of protection, ''clinical data' as including "all relevant clinical and socioeconomic data disclosed by the patient and others, as well as observations, findings, therapeutic interventions and prognostic statements generated by the members of the healthcare team.' Legislative proposals, however, define health care information in different ways. The Model State Legislation on Confidentiality for Health Care Information of the American Medical Association refers to ''confidential health care information, ' defining it as information relating to a person's health care history, diagnosis, condition, treatment, or evaluation, regardless of whether such information is in the form of paper, preserved on microfilm, or stored in computer-retrievable form. The language of this legislation is particularly helpful because it provides that health care records be recognized by law when in electronic form.

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

- relates to a patient's health care; or
- is obtained in the course of a patient's health care from a health care provider, from the patient, from a member of the patient's family or an individual with whom the patient has a close personal relationship, or from the patient's legal representative,

This language acknowledges health care information in its broadest terms as being information relating to or collected in the course of a patient's health care, and does not limit it to where it resides. Arguably, health care information (beyond the contents of the medical record) located in such places as student files, pharmacy comput-

---

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

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

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

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

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

[12] Ibid.

ers, public health agencies, and lawyers offices is covered by this definition. The scope of AHIMA's proposed legislation would provide coverage to information as it flows through a complex computer network through which it is accessed by a variety of primary and secondary users.

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

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

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

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

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

The AHIMA Model Legislation provides that anyone who requests or obtains health care information under false or fraudulent pretenses is subject to a $10,000 from or imprisonment for 6 months. Anyone who obtains health care information fraudulently or unlawfully and intentionally uses, sells, or transfers the information for some monetary gain is subject to frees of not more that $50,000 and imprisonment for 2 years. The

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

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

AHIMA Model Legislation also provides for civil remedies and monetary penalties. Among the civil money penalties provided for is a from of not more that $1,000,000 if it is found that violations of the provisions have occurred in such numbers or with such frequency as to constitute a general business practice. In the discussion about health care information privacy, commentators and stakeholders indicate that for legislation to be meaningful, penalties for improper access, possession, brokering, disclosure, or sale of information must be stringent enough to deter perpetrators.[15] Provisions or penalties such as those set forth in the AHIMA Model Legislation might be more likely to deter information brokers who might otherwise include frees and penalties in their cost of doing business.

Provision 3: *Establish requirements for informed consent.*

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

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

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

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

---

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

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

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

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

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

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

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

> We keep a record of the health care services we provide for you. You may ask us to see and copy that record. You may also ask us to correct that record. We will not disclose your record to others unless you direct us to do so or unless the law authorizes or compels us to do so. You may see

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

[19] The Federal Privacy of Medical Information Act (H.R. 5935), introduced before the 96th Congress in 19 80, provided that a medical care facility shall, on request, provide any individual with a copy of the facility's notice of information practices and shall post in conspicuous places in the facility such notice or a statement of availability of such notice and otherwise make reasonable efforts to inform patients (and prospective patients) of the facility of the existence and availability of such notice. Sec. 113(b).

your record or get more information about it at. . , .[20]

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

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

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

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

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

---

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

1) the disclosures of medical information that the facility may make without the written authorization of the patient;

2) the rights and procedures . . . including the right to inspect and copy medical information, the right to seek amendments to medical information and the procedures for authorizing disclosures of medical information% and the procedures for authorizing disclosures of medical information and for revoking such authorizations; and

3) the procedures established by the facility for the exercise of these rights.

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

and formal authorization before information will be released.

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

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

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

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

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

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

Brannigan's approach to protecting privacy in clinical information is through the use of 'technical tools. ' '[23] These tools include both "machine-based" and ''people-based" precautions, including concepts such as 'need to know, ' encryption,

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

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

audit trails, read/write limitations, physical keys, and passwords .24

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

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

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

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

In addition, the system might include:

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

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

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

One approach to addressing the problem of maintaining privacy in computerized medical records is the establishment of a committee on health care information privacy. Such a committee could be modeled in some aspects on proposals for a data protection board.[26] legislation alone cannot address all of the privacy problems created as a result of quickly changing and developing computer technology. A committee could serve a more dynamic function and could assist in implementing the health care information privacy policies set out in legislation. Data protection

---

24 Brannigan notes that one characteristic of these tools is that they can pre-exist any legal structure or be established as the result of one. ''[T]he legal system can either follow or force a technology." Ibid.

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

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

boards have been instituted in several foreign countries, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Iceland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia.[27]

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

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

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

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

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

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