

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

Collection/Record Group: Clinton Presidential Records

Subgroup/Office of Origin: National AIDS Policy Office

Series/Staff Member: Todd Summers

Subseries:

OA/ID Number: 21080

FolderID:

Folder Title:

Issues - Privacy - HHS [Health and Human Services]

Stack:

S

Row:

66

Section:

6

Shelf:

3

Position:

3

CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION



**Recommendations of the Secretary of Health and Human Services, pursuant
to section 264 of the Health Insurance Portability and Accountability Act of
1996**

Submitted to:

**The Committee on Labor and Human Resources and the Committee on Finance of the
Senate**

**The Committee on Commerce and the Committee on Ways and Means of the House of
Representatives**

On September 11, 1997

CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION

Recommendations of the Secretary of Health and Human Services, pursuant to section 264
of the Health Insurance Portability and Accountability Act of 1996

I.	INTRODUCTION	2
A.	Background	3
B.	Why Federal Legislation is Needed	5
C.	Recommendation for Establishing Federal Privacy Standards	8
D.	Principles	9
E.	Boundaries -- Recommended Scope of A Federal Privacy Law	10
F.	Security	13
G.	Consumer Control	14
H.	Accountability	14
I.	Public Responsibility	15
J.	How Federal Privacy Legislation Should Relate to Other Laws	17
K.	Particular Classes of Information	19
II.	THE RECOMMENDATIONS	19
A.	Coverage	19
B.	Basic Requirements	26
C.	Patient Awareness and Control	31
D.	Disclosures Authorized by the Patient	39
E.	Other Disclosures	43
F.	Specialized Classes of Persons and Entities	66
G.	Relationship to Other Law	71
H.	Enforcement	77
I.	Administration	80
III.	CONCLUSION	82

CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION

Recommendations of the Secretary of Health and Human Services, pursuant
to section 264 of the Health Insurance Portability and Accountability Act of
1996

I.

INTRODUCTION

Every day, our private health care information is being collected, shared, analyzed and stored with few legal safeguards. There was a time when our health care privacy was protected by our family doctors -- who kept hand-written records about us sealed away in big file cabinets. Today, revolutions in our health care delivery system mean that we have to place our trust in entire networks of insurers and health care professionals. The computer revolution means that our family secrets travel quickly from doctors to hospitals to insurance companies -- and cannot be protected by simply locking up the office doors each night. And, revolutions in biology mean that a whole new world of genetic tests have the potential to help either prevent disease or reveal our most personal secrets.

Right now, the way we currently protect the privacy of our medical records is erratic at best -- dangerous at worst. It is time for our nation to enact federal legislation to protect the age-old right to privacy in this new world of progress. This report recommends that Congress enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who serve them. Specifically, a federal privacy law should:

- impose new restrictions on those who pay and provide for care, as well as those who receive information from them. It should prohibit disclosure of patient-identifiable information except as authorized by the patient or as explicitly permitted by the legislation. Disclosures of identifiable information should be limited to the minimum necessary to accomplish the purpose of the disclosure, and should be used within an organization only for the purposes for which the information was collected.
- provide consumers with significant new rights to be informed about how their health information will be used and who has seen that information. Providers and payers should be required to advise patients in writing of their information practices. Patients should be able to see and get copies of their records, and propose corrections. A history of disclosures should be maintained by providers and payers, and be made accessible to patients.
- provide for punishment for those who misuse personal health information and redress for people who are harmed by its misuse. There should be criminal penalties for obtaining health information under false pretenses, and for knowingly disclosing or using medical

information in violation of the Federal privacy law. Individuals whose rights under the law have been violated should be permitted to bring an action for damages and equitable relief.

We are at a decision point. Depending on what we do, revolutions in health care, biotechnology, and communications can hold great promise or great peril. We must ask ourselves: Will we harness these revolutions to improve, not impede, health care? Will we strengthen, not strain, the very lifeblood of our health care system -- the bond of trust between a patient and a doctor. When all is said and done, will our health care records be used to heal us or reveal us?

Without safeguards to assure that obtaining health care will not endanger our privacy, public distrust could turn back the clock on progress in our entire health care system. Instead, we must keep our eye on the future, and act today.

A. BACKGROUND

The American people expect, and are entitled to, confidential, fair, and respectful treatment of health information about themselves. This report recommends that the Congress enact legislation requiring that treatment.

The need for such legislation is found in the rapid changes in the ways that health care is provided, documented, and paid for in the United States. These changes pose a challenge to American values that are both complementary and competing.

On the one hand, patients have a legitimate need for assurance of the confidentiality that permits them to be frank with their physicians about their health conditions and behavior. That assurance is fundamental to effective diagnosis, treatment and healing, and to the privacy that we in the United States cherish as essential to personal freedom and well-being.

On the other hand, participants in the health care system -- insurers, governments at all levels, managed care organizations -- have legitimate needs for access to health records in performing their roles in the system. Furthermore, those pursuing broad social purposes -- medical researchers, public health workers, governmental policy makers seeking to contain health care costs -- rely on the availability of data arising from these private transactions. Local public health agencies use health records to identify outbreaks of infectious disease, and to trace the source of infections like the recent *e. coli* infections. Researchers have used health records to help us fight childhood leukemia and uncover the link between DES and reproductive cancers.

Until comparatively recently, any tension between these needs for confidentiality and access was resolved directly between patients and their physicians. They conducted an essentially one-on-one relationship, in examination, treatment and payment, and, with some exceptions, could limit access to information about the patient. The paper records once kept under the control of

physicians are giving way to computerized information which is increasingly stored far from its source -- the patient and the physician -- in forms and even locations of which they may have only imperfect understanding. Even physicians may be frustrated in their traditional role as patient advocates by the complexity of the systems that process their patients' information.

Moreover, patients may have little if any contact with some of the doctors and payers involved in their care. The result has been a weakening of the traditional, if often informal, controls that patients and physicians previously exercised to protect patient information.

The President spoke to the importance of these concerns in his commencement address at Morgan State University on May 18, 1997. He said that "technology should not be used to break down the wall of privacy and autonomy free citizens are guaranteed in a free society". He acknowledged the special concerns surrounding health records in his call for enhanced protections for privacy in the face of new technological reality, when we are facing "the frightening prospect that private information -- even medical records -- could be made instantly available to the world."

Our Nation's participation in the Global Information Infrastructure (GII) has sharpened the issues, and our plans for that participation include attention to privacy protection. The statement of the President and Vice-President, *A Framework for Global Electronic Commerce* reflects this concern and commitment:

Americans treasure privacy, linking it to our concept of personal freedom and well-being. Unfortunately, the GI's great promise -- that it facilitates the collection, re-use, and instantaneous transmission of information -- can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.

The concern about confidentiality of health information appears against a backdrop of more general concern about privacy, well expressed by Alan Greenspan, the Chairman of the Federal Reserve Board:

The fears of invasion of privacy, as a consequence of inexorable forces seemingly out of the control of the average American, has risen to a major public policy issue. (Speech, Conference, "Privacy in the Information Age", Salt Lake City, Utah, March 7, 1997)

These concerns are not confined to the United States. The European Union (EU) has addressed the issue, and the EU data protection directive requires member States to "protect the

fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to processing of personal data".¹

B. WHY FEDERAL LEGISLATION IS NEEDED

The existing legal structure does not effectively control information about individuals' health. Federal legislation, establishing a basic national standard of confidentiality, is necessary to provide rights for patients and define responsibilities for record keepers. Today, patients often sign blanket authorizations allowing use of their medical information in order to obtain treatment or payment for care. These authorizations may not really protect us, in part because they do not provide useful information about how our health records will be used, who will see them, or how we can get access to them. Such authorizations are not always voluntary -- if we do not sign the blanket authorization, we may sacrifice the ability to receive care or insurance benefits. In addition, as the health care system becomes more integrated and more computerized, it is becoming difficult to determine the appropriate person or place where our health information can be accessed or controlled.

For these reasons, we are recommending that Congress replace the ineffective use of authorizations with a system of Federal legislative controls on the use of health information collected by health care payers and providers. As described below, Federal legislation should authorize sharing information for health care treatment and payment, and prohibit use of that information for most other purposes. Such legislation should also provide consumers with specific rights to know how their information will be used, to get access to that information, to request correction of errors, and to know who has seen their medical information.

Informal
Consent

Before turning to the details of our recommendations, however, it is important to describe the current situation, and the general consensus that Federal action is needed.

Current Protections are Inadequate. Today the legal control of health information is, in general, a matter of State law. Limited Federal law covers specialized classes of information such as information about substance-abuse patients and information gathered in some Federally funded programs. The Privacy Act of 1974 provides some procedures and protections for records, including health records, held by Federal agencies.

¹The directive requires EU States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to processing of personal data". (Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 25, ¶ 1 (Eur. O.J. 95/L281)).

All States have legal controls on the use and disclosure of health information, including a few comprehensive acts similar in broad outline to the Federal legislation we recommend here. Two States have enacted the Uniform Health-Care Information Act recommended by the National Conference of Commissioners on Uniform State Laws in 1985.² Many State laws protect special classes of health information, about HIV infection and AIDS patients and about mental health patients, for example. Some State case law imposes confidentiality duties.

These State laws vary greatly in scope and strength, and the situation has been described as "a morass of erratic law, both statutory and judicial, defining the confidentiality of health information."³

The Health Care Information System Is Increasingly Interstate. The health care system, particularly its information component, is very much an interstate activity, and will continue to develop in that direction. Computerization and telecommunications render the concept of "location" of information nearly meaningless. Patients receive care in more than one State, information about them is moved electronically across State borders to obtain payment (often through and to places remote from the patient and the provider), and providers operate across many States. In its administrative simplification requirements, the Health Insurance Portability and Accountability Act of 1996 calls for uniform standards for electronic transactions in health administration precisely because separate standards developed at other than the national level are not workable.

There is continuing movement toward a computer-based patient medical record, with national standards for content and format, and the possibility of ready interstate transmission as needed for patient care. A major impetus toward adopting this type of record was a report of the Institute of Medicine in 1991 that recommended adoption of the computer-based patient record as the standard for all patient care records.⁴

Likewise, increasing use of telemedicine means that patient information will often cross State lines, sometimes in real-time delivery of care. This promising development is an important facet

²9 Part I, U.L.A. 475 (1988 and Supp. 1996)

³Workgroup for Electronic Data Exchange, *Report to the Secretary of U.S. Department of Health and Human Services* Appendix 4, Confidentiality and Antitrust Issues 5 (1992). For other analyses of the State law situation see Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. Rev. 255 (1984); Lawrence O. Gostin, *Health Information Privacy*, 80 Cornell L. Rev. 101 (1995); Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law* § 7-3 (1996).

⁴Richard S. Dick and Elaine B. Steen, eds., *The Computer-Based Patient Record: An Essential Technology for Health Care* (1991). A revised version of this report is expected in the autumn of 1997.

of the National Information Infrastructure because of its potential to provide greater access to quality health care for all Americans, especially those living in rural and remote areas.

The Problems Are Urgent. The need for Federal protection is not theoretical; it is real and it is urgent. In a major American city, a local newspaper published medical record information about a Congressional candidate's attempted suicide. But it is not just public figures such as the Congressional candidate or Arthur Ashe (whose HIV status was published in a newspaper without his permission) who are at risk:

- The director of a work site health clinic operated by a large manufacturing company testified before the National Committee on Vital and Health Statistics that he was frequently pressured to provide personal health information about his patients to their supervisors.
- Until recently, at a Boston-based HMO clinic, all employees could tap into patients' mental health treatment records in the clinic's computer. In Colorado, a medical student copied health records at night and sold them to medical malpractice attorneys.
- Medical records were dumped in a parking lot after a psychiatric clinic in Louisiana was sold.

Inappropriate disclosure of personal medical information is not the only problem we are facing. Errors in health information, errors that can have profound financial effects, are often too difficult to correct. Such inappropriate handling of medical information can and should be prevented.

Calls for Federal Legislation. Numerous analyses over several years by government, industry, and professional groups have identified serious gaps in protections for health information, especially in the unregulated exchange of data, and have recommended Federal legislation to close them. There also has been significant Congressional action toward this goal, including several comprehensive health privacy bills introduced by Senators Bennett and Leahy, Representative McDermott, and Representative Condit. The fact that Congress, in the Health Insurance Portability and Accountability Act, mandated that the Department of Health and Human Services produce these recommendations is further evidence that the Congress understands that the time has come for action.

- Earlier this year, the National Committee on Vital and Health Statistics held hearings and advised on this issue. After six days of hearing witnesses from the full spectrum of public and private constituencies concerned with privacy, consumer interests, and

operation of the health care system, the Committee strongly recommended that the 105th Congress enact a health privacy law.⁵

- The Office of Technology Assessment, in a study of privacy and medical information, noted that lack of legislation "allows for a proliferation of private sector computer databases and data exchanges without regulation, statutory guidance, or recourse for persons wronged by abuse of data."⁶
- A study of regional health data networks by the Institute of Medicine recommended Federal privacy legislation.⁷

C. RECOMMENDATION FOR ESTABLISHING FEDERAL PRIVACY STANDARDS

We thus conclude that Federal legislation, establishing a basic national standard of confidentiality, is necessary to provide rights for patients and define responsibilities for record keepers. Such legislation should provide clear guidance and significant incentives for the confidential, fair, and respectful treatment of personal information that the public expects. It should encourage administrative, technological, and management choices in design of health information systems to these ends. And it should provide redress to those adversely affected by misuse of information.

⁵The National Committee on Vital and Health Statistics, an advisory committee to the Secretary of Health and Human Services, is established by the Public Health Service Act § 306(k), 42 U.S.C. § 242k(k), and its membership was expanded to include persons distinguished in "privacy and security of electronic information" by the Health Insurance Portability and Accountability Act of 1996. In the course of its consultation on these recommendations, its Subcommittee on Privacy and Confidentiality held six days of hearings on health privacy during the first two months of 1997. Witnesses included health care providers, researchers, public health authorities, Federal and State oversight agencies, accreditation organizations, insurers, claims processors, pharmaceutical manufacturers, Federal agencies, law enforcement agencies, and patient and privacy advocates. (Health Privacy and Confidentiality Recommendations of the National Committee on Vital and Health Statistics, Approved on June 25, 1997)

⁶U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information* 44 (1993).

⁷Molla A. Donaldson and Kathleen N. Lohr, eds. *Health Data in the Information Age: Use, Disclosure and Privacy* 190 (1994).

We are aware that our recommendations come at a time of continuing, rapid change in the health care system and its information components. The standards for administrative simplification that the Department will soon publish, under the Health Insurance Portability and Accountability Act of 1996, will in themselves lead to new developments in the transfer and use of information. In addition, the boundaries between health information and other information are blurring. Marketing uses of health information and health uses of marketing information may ultimately make this activity a subject for legislation. New technologies and new uses, unthought of before now, will present new issues and new concerns. These possibilities may well warrant legislative attention in the future, and bear careful watching.

Aware of these contingencies, and of the need they may present for further legislative attention, we nevertheless recommend that the Congress enact legislation now, based on what we know now. Today, we should move forward with legislation that protects the heart of the health care system -- those who provide and pay for health care, and those who get information from them. Delay will leave the public unprotected as more information flows to more places.

D. PRINCIPLES

Our recommendations are founded on five key principles:

Boundaries. An individual's health care information should be used for health purposes and only those purposes, subject to a few carefully defined exceptions. It should be easy to use information for those defined purposes, and very difficult to use it for other purposes. Federal health record confidentiality legislation should impose a legal duty of confidentiality on those who provide and pay for health care, and on other entities that receive health information from them.

Security. Organizations to which we entrust health information ought to protect it against deliberate or inadvertent misuse or disclosure. Federal law should require such security measures.

Consumer Control. Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them. Our recommendations significantly strengthen the ability of consumers to understand and control what happens to their health care information.

Accountability. Those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal recourse. Federal law should provide new sanctions and new avenues for redress for consumers whose privacy rights have been violated.

Public Responsibility. Individuals' claims to privacy must be balanced by their public responsibility to contribute to the common good, through use of their information for

important, socially useful purposes, with the understanding that their information will be used with respect and care and will be legally protected. Federal law should identify those limited areas in which our public responsibilities warrant authorization of access to our medical information, and should sharply limit the uses and disclosure of information in those contexts.

Federal privacy legislation should not require any disclosure of information, except to patients who ask to see their own records. The recommended allowable disclosures are just that -- allowable. Thus, for disclosures that are not compelled by other law, providers and payers should be free to disclose or not, according to their own policies and ethical principles. We offer these recommendations as a basic set of legal controls. But ethics and professional practice will, in many cases dictate more guarded disclosure policies.

Similarly, where our recommendations would permit disclosure, they are not intended to create any new legal basis for refusing to disclose if such disclosure is required by other law.

Finally, our recommended standards are not intended to preempt or supersede other laws -- State or Federal -- that are more protective of individual privacy.

The effect of implementing our recommendations would be that some current uses of information could not continue without patient authorization. Some organizations that get information with ease now may not be able to get information without patient authorization, or without meeting new requirements. We have designed the requirements to serve patients.

These recommendations must steer a course between two extreme convictions: that privacy is already so compromised that attempts to control health information are futile, and that privacy is so weighty a value that we must reverse our efforts to use information effectively. Legislation must, therefore, strike a balance that permits socially important uses of information while protecting the privacy of people who seek care and healing. We believe our recommendations find that balance.

The remainder of this Introduction is a summary of the scope and content of what we believe a Federal health information privacy law should provide. A more detailed description of our specific recommendations for the rights of patients and the obligations of those who hold health information follows. Our recommendations are framed as expressions of basic policy for the major choices in designing such legislation. We appreciate the difficult choices and complex accommodations required to make Federal health privacy legislation a reality. We look forward to working closely with the Congress in developing such legislation.

E. BOUNDARIES -- RECOMMENDED SCOPE OF A FEDERAL PRIVACY LAW

There are four situations in which health information is collected, disclosed, or used, and that we recommend be addressed by Federal health privacy legislation:

Provision of and Payment for Health Care. A Federal health privacy law should focus on health care payers and providers and the information they create and receive for the provision and payment of health care, and on those who receive information from those payers and providers. Providers and payers are the foundation of the health care system, and the primary creators and collectors of health information. The provisions of a Federal privacy law generally should apply to information about a patient collected in the provision of health care services or in the payment for health care services.

A Federal privacy law should apply uniformly, regardless of the setting in which health care is provided. A person seeking treatment should be able to discuss his or her medical condition freely, with confidence that the information will be protected, whether treatment is sought from a private physician or hospital, a company doctor, or a community health center. Similarly, the law should apply uniformly to all such information, whether the information is oral or written, on paper or in a computer.

A Federal health privacy law should limit the ways providers and payers can use identifiable health information. However, it need not cover information that individuals voluntarily provide about themselves directly to parties other than providers or payers, such as retailers or marketers.

Health care research that includes the delivery of health care should be included in Federal privacy protections. Information obtained in this context should be protected by a Federal privacy law. Research that does not involve care, but which is based on medical records obtained from providers and payers, should also be protected, since the information is obtained directly from the health care system.

Employers that render on-site health care for their employees, or provide health benefits through a self-funded health plan, are acting as providers and payers, and in this context should be covered by a health privacy law. They should be able to collect and use identifiable health information for health care and directly related purposes, but should not use the information they collect a providers and payers for other purposes, such as hiring and firing, placement and promotions.

Health information often is obtained from individuals for purposes other than the provision of or payment for health care, and we recommend that these situations be addressed by other legislation. Thus, these recommendations do not extend to the results of a fitness-for-duty examination. Nor do our recommendations address the need for protection of genetic information in Federal and State DNA banks and DNA data banks for casualty identification or criminal investigation,

or of information generated in workplace drug-testing programs. Some existing uses of health information should not be affected at all, such as reporting of birth and death and reporting of abuse such as child abuse. The confidentiality risks of these collections of information should be (and often are) addressed by legislation specific to them.

We recognize that distinctions among the various holders of health information are not always clear. We are particularly concerned about automobile and similar types of insurance that include a health coverage component. While these insurers may not be labeled "health insurers," as a practical matter they obtain the same information in the same ways, and serve the same functions, as health insurers. Similarly, there may be some grey areas regarding when an employer is functioning as a provider (and thus covered by a Federal privacy law) and when not. These are areas that would benefit from public debate and additional fact-finding. We continue to review specific instances, and may ultimately find that some information not now recommended for protection can and should be included in a Federal privacy law.

Similarly, we recognize that the collection, development, and use of information about health matters by entities other than providers and payers can present serious privacy hazards. It may well be appropriate to impose confidentiality restrictions in those contexts. While we now recommend a Federal health privacy law limited to health information held by providers and payers (and those receiving such information from them), we also believe that the Administration and Congress must continue to examine the hazards to privacy when health information is held in other settings, and consider ways of controlling those hazards.

Service Organizations. Providers and payers do not act alone. They engage other organizations to assist in processing health information. These "service organizations" may be claims processors, pharmacy benefits managers that provide information to pharmacists about coverage and drug interactions, or similar organizations that process information to help make the health care system work better. These organizations should be bound by the same restrictions that apply to the providers and payers from which they obtain the health information. Service organizations have access to patients' health information as an integral part of the provision of and payment for health care, and should be bound by a Federal health privacy law.

Limited Disclosures for National Priorities. Federal health privacy legislation should also allow certain uses of identifiable health information needed to support national priority activities. In exchange for this access to information, legislation also should place strict boundaries around the use and redisclosure of that information to ensure that it is used for the identified priority purpose only. The major national priorities which we recommend for this treatment are public health, oversight of the health care system, research, and law enforcement. For these activities, it is not always possible to obtain permission and, in many cases, doing so would create significant obstacles in our efforts to fight crime, protect public health, or understand disease.

However, along with access should come the duty to use that information only subject to legislative restrictions on how the information may be used and disclosed, tailored to the particular situations.

Disclosure with Authorization. Sometimes a patient will authorize a provider or payer to disclose information to a third person not directly subject to the Federal health confidentiality legislation that we recommend. In these cases, the patient should be able to enforce an agreement with that third person about how the information will be used. Federal law should impose an enforceable obligation on the recipient to use the information only in accord with the agreement made with the patient at the time of the authorization.

For example, if a potential employer requires health information as part of a background check for security purposes, the applicant can authorize his or her health care providers to disclose the information. But the employer's use of the information should be governed by the employer's statement of how it will use the information, and that agreement should be enforceable.

F. SECURITY

We recommend that a Federal health privacy law impose new restrictions on health care payers and providers who create and receive health information, and on those who receive information from those payers and providers. Specifically:

- Patient-identifiable information should not be disclosed except as authorized by the patient or as explicitly permitted by the legislation.
- Those holding such information should be required to implement security measures to protect the information against reasonably anticipated threats.
- All-disclosures of identifiable information should be limited to the minimum necessary to accomplish the purpose of the disclosure.
- Patient information should be used within an organization only for purposes reasonably related to the purposes for which the information was collected.
- A patient's authorization to disclose information should have to meet specific requirements.
- A provider or payer should not be allowed to condition treatment, payment, or coverage on a patient's agreement to disclose health information unless the information is needed for treatment, coverage, or payment purposes.
- Those receiving information through a patient's authorization should be required to abide by the terms of the authorization agreement, or face civil liability.

The attached recommendations provide the details for how such restrictions might operate. Many of these recommended rules would simply codify sound professional practices. For example, a provider should be able to use identifiable health information for mailing reminders to patients to schedule appointments. It should not be able -- absent patient consent -- to make available its patient list to a health company for use in a direct mailing announcing a new product or service (even if that product or service might benefit the patient). Providers and payers should be limited in their internal use of information, so that, for example, employers who obtain health information through their operation of self-insured health plans (i.e. as payers) should be prohibited from using that information for personnel decisions.

G. CONSUMER CONTROL

Americans should know what rules protect their health records, how those records will be used and shared, how they can obtain their records and, if necessary, how they can correct errors in their records. We recommend that Federal law provide consumers with significant new rights to be informed about how their health information will be used and who has seen that information. Specifically:

- Providers and payers should be required to advise patients in writing of their information practices. This notice should state clearly how the information will be used, and should also explain the patient's rights to limit disclosures.
- Patients should be able to see and get copies of their records, and propose corrections.
- A history of disclosures should be maintained by providers and payers, and be made accessible to patients.

Our intent is to incorporate basic fair information practices into the health care setting. The attached recommendations provide details for how to make these consumer controls real.

H. ACCOUNTABILITY

The requirement to safeguard information must be supported by real and severe penalties for violations. Federal legislation should include punishment for those who misuse personal health information and redress for people who are harmed by its misuse. Specifically:

- There should be criminal penalties (including fines and imprisonment) for obtaining health information under false pretenses, and for knowingly disclosing or using medical information in violation of the Federal privacy law.
- Penalties should be higher when violations are for monetary gain.

When there is a pattern or practice of unauthorized disclosure or other violations, there should be civil monetary penalties.

Any individual whose rights under the law have been violated, whether negligently or knowingly, should be permitted to bring an action for actual damages and equitable relief. For knowing violation attorney's fees and punitive damages also should be available.

Only if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibilities seriously.

I. PUBLIC RESPONSIBILITY

A Federal health privacy law should permit limited disclosures of health information without patient consent for specifically identified national priority activities. We have carefully examined the many uses that the health professions, related industries, and the government make of health information, and we are aware of the concerns of privacy and consumer advocates about these uses. The allowable disclosures and corresponding restrictions we recommend reflect a balancing of privacy and other social values.

Specifically, in addition to disclosure for health care and payment purposes discussed above, we recommend that Federal legislation authorize disclosure of health information without explicit patient consent for four national priority activities. Recipients of information under such a legislative authorization should also be bound by restrictions on use and further disclosure of the information, tailored to their particular circumstances.

Oversight of the Health Care System (including audit, investigation, quality assurance, and licensure). Combating fraud, abuse, and waste in health care and related payment programs is a major national priority. In addition, we have both legal and ethical duties to improve the quality of health care and records review is essential to this important task. We recommend that the legislation not add additional restrictions to access to health information for these purposes. No new judicial or administrative procedure should be required before oversight agencies can see health records, or use them against patients, providers, and others for wrongdoing in health or related programs. At the same time, existing legal constraints that govern access to or use of such information by oversight organizations should remain in place. We are also recommending criminal penalties for obtaining health information under false pretenses.

For Public Health, and in Emergencies Affecting Life or Safety. The importance of public health and emergency medical activities to our health and safety cannot be overstated. Health information is necessary for tracing the source of rapidly spreading infectious diseases, finding links between diseases and their causes, and rendering appropriate medical care to victims in emergencies. We recommend that there be no new procedural burdens in the way of these

priority, often urgent, activities. At the same time, public health workers should be prohibited from redisclosing that information for any other purpose.

For Health Research. Research is essential to our health care. Federal law should permit use of information for research without consent under carefully-defined circumstances, and should also include safeguards, including restrictions on redisclosure, to ensure that individual subjects are not harmed. Federal requirements should include a determination by an institutional review board that the research does not involve more than minimal risk, that the absence of consent will not harm the participants, and that the research would be impracticable if consent were required.

We also propose accommodating the special needs of clinical trials. Generally, patients should have access to their own records. For clinical trials, however, we recommend a limited exception to permit agreements that research subjects typically make, such as to forego access to their trial-related records for the duration of their participation in the trial, as long as they are consistent with Federal rules for the protection of research subjects.

Pursuant to Other Laws or Court Orders, such as: to Law Enforcement Authorities, to State Health Data Systems, and in Court Proceedings. Law enforcement agencies need access to health information for many purposes. We recommend that this Federal health privacy law not alter current practices; that is, it should neither expand nor contract current laws governing disclosure of health information to law enforcement authorities. In many instances, law enforcement authorities today can obtain, share, and use health information without patient consent and without legal process. We are not recommending changes to these practices. Similarly, existing legal constraints on law enforcement access to and use of medical information should remain in place.

We recognize that new issues are raised by the search capabilities of computerized records, and that there are arguments in favor of new restrictions to address these possibilities. However, until more experience is gained with the uses of computerization of these records, and the types and frequency of requested searches, it is premature to change existing law in this area.

J. HOW FEDERAL PRIVACY LEGISLATION SHOULD RELATE TO OTHER LAWS

Any Federal legislation controlling health information must be understood in the context of other State and Federal laws that also address, either incidentally or directly, the confidentiality of health information. In short, we recommend that existing confidentiality laws at both State and Federal level which provide more protection remain in force. A new Federal privacy law should provide a basic level of protection for everyone -- a "floor" of protection -- without reducing other protections.

State Law. As noted above, there exists today a patchwork of State health privacy laws. While some are comprehensive and strong, the array of protections we recommend here would, in general, be stronger than most existing State law.

We recommend that Federal health privacy legislation supersede State law that is less protective than the Federal law. If either the Federal or State law forbids a disclosure, the disclosure should not be made. Thus, the confidentiality protections should be cumulative, and the Federal legislation should provide "floor preemption."

We make this recommendation with the recognition that a single national standard may be preferable from the administrative simplification perspective, and that some privacy interests might also be better served thereby. However, at this time, the freedom of States to protect their citizens' privacy through their own legislation is more important than the benefits of standardization that totally preemptive Federal legislation would confer. The attention several States have given to this issue should be respected. Many States have statutes to protect information about HIV infection and AIDS patients, and about mental health patients, designed after wide public debate to suit local needs. In addition, the Federal government can clearly learn from the experiences of States as they respond to the complex task of protecting patient information in a rapidly changing environment.

Other Federal statutes that afford protection to liberty, privacy, and consumers' rights generally do not displace stronger State laws. At present, the goals of this proposal argue that it not break that tradition.

In addition, Congress expressed a preference for leaving stronger State laws in place in the Health Insurance Portability and Accountability Act of 1996. That Act calls for the Secretary of Health and Human Services to impose confidentiality controls on electronic transaction systems if Congress does not legislate on confidentiality by August 1999, and directs that any such controls not supersede State law with more stringent requirements.⁸ Likewise, the standards for administrative simplification of health financial and administrative transactions, which that Act

⁸Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264(c)(2), 110 Stat. 1936, 2033 (1996). Congress has provided for confidentiality protection for a limited class of information if legislation is not enacted.

If Congress does not enact legislation on standards for privacy of health information *transmitted in connection with financial and administrative transactions* (i.e. the information subject to the standards to be developed under section 262) within 36 months, the Secretary of HHS must issue regulations with privacy standards for *these transactions* within 42 months of enactment (§ 264(c)(1)). This is timed to coincide with the effective date of the standards under section 262.

requires the Secretary of HHS to promulgate, may not supersede stronger State confidentiality laws.⁹

Privacy needs, developments in health data systems, and the interests of nationwide administrative simplification for health transactions may ultimately justify preemptive Federal legislation. But, at least at present, as the National Committee on Vital and Health statistics noted, "this issue need not be treated as a single problem with a single solution."¹⁰

If the Congress enacts Federal legislation leaving State controls in place, the impact of the respective laws on individual privacy rights and on effective use of health information bears careful watching. To the extent that dual regulation impairs health care or the operation of information and payment systems, poses risks to confidentiality arising from misunderstanding of the applicability of multiple laws, or creates uncertainty in patients about rights and redress, consideration of additional action, such as developing a single national law or preempting State laws in particular areas, may be warranted.

Federal Law. Similarly, we recommend that a Federal privacy law not limit or reduce other Federal legal protections that control how information about individuals is disclosed or used. As with State law, Federal privacy protections should be cumulative.

For example, even where the recommended Federal privacy law would allow a disclosure without patient consent or judicial process, it should not obviate the need to comply with other Federal statutes that do require consent or judicial process. Nor should it diminish any rights, of patients or record holders, to challenge disclosures under other Federal law. If another Federal law requires legal process, or specific showings, prior to a disclosure, a record holder should remain obligated to observe those requirements.

For Federal health records, the records management requirements and subject access provisions of the Privacy Act of 1974 should continue to apply. But we recommend that the Privacy Act's disclosure provisions be replaced by the general health information disclosure restrictions we recommend, to the extent that the latter are more stringent than the Privacy Act.

K. PARTICULAR CLASSES OF INFORMATION

No segregation
At present, we recommend that Federal health confidentiality law treat all types of health information alike. The intent is to provide a meaningful minimum floor of privacy protections in

⁹Social Security Act § 1178(a)(2)(B), added by section 262 of the Health Insurance Portability and Accountability Act of 1996.

¹⁰Health Privacy and Confidentiality Recommendations of the National Committee on Vital and Health Statistics, Approved on June 25, 1997

Federal law for all types of health information. We recognize, however, that there is a great deal of support for providing additional protection to certain types of health care information that people feel to be particularly sensitive. For example, Federal and State laws already provide stronger protections for certain information, (such as information about HIV status, substance abuse patient information, and mental health records), and we recommend that these standards remain in place. We further recognize that additional types of particularly sensitive information may be identified for special protection in the future, and look forward to working with the Congress in determining when such protections are appropriate.

* * * *

The following are our recommendations for the contents of a federal health privacy statute. There will be many important details to be discussed, both in drafting legislation and then in developing implementing regulations. The following recommendations are not intended to address privacy policy at that level of detail. Rather, the following are statements of principle and policy that describe our recommended framework for federal health privacy legislation. We look forward to working with the Congress on a bi-partisan basis to advance these principles and enact Federal legislation that provides a basic set of rights with respect to health information to all Americans. This is an essential beginning.

II. THE RECOMMENDATIONS

A. COVERAGE

1. PROVIDERS AND PAYERS, AND THOSE WHO RECEIVE INFORMATION FROM THEM

We recommend that Federal health privacy legislation apply primarily to health care providers and payers.

We recommend that persons receiving information under the provisions of such legislation without patient authorization for health oversight, public health, research, State data system purposes be subject to the requirements of the legislation.

law
enforcement
absent?

We recommend that health care providers be defined as persons who receive, create, use, or maintain, health information while providing health care in the ordinary course of business or practice of a profession, pursuant to license, certification, registration, or other legal authorization.

We recommend that payers be defined to include persons who pay for health care through contracts of insurance or in connection with employment, and government programs that pay for care under a benefit plan.

The legislation we recommend should apply in the first instance to providers of health care and payers for health care. They are at the heart of health care, and typically receive information directly from patients and generate health information. They are often one and the same.

In turn, others who receive health information under the provisions of the legislation without patient authorization should be bound by its requirements. They are referred to as "those receiving health information under the provisions of the law without patient authorization."

Providers are persons -- individual and institutional -- who receive, create, use, or maintain, health information while providing health care (including preventive health services) in the ordinary course of business or practice of a profession, pursuant to license, certification, registration, or other legal authorization.

Health care payers pay for health care pursuant to advance agreements or statutory obligations -- the range of entities commonly described as "plans." They may include licensed insurance companies, hospital or medical service corporations, health maintenance organizations, or other entities licensed or certified by a State to provide health insurance or health benefits. They include employee welfare benefit plans and other arrangements that provide health benefits, whether or not funded through the purchase of insurance policies or contracts. They include public programs that pay for health care under a health benefit plan, such as Medicare, Medicaid, the health programs of the Veterans Health Service, and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS). The term should not be defined to include individuals and families who pay for their own care.

The definition does not encompass liability insurers who receive health information, as needed, pursuant to claimants' authorization. Nor does it include life insurers, who receive information, with the patient's authorization, not as part of health care or payment, but to make underwriting decisions.

We are making no recommendations with respect to including workers' compensation under Federal health privacy legislation at this time. Although workers' compensation carriers receive health care information in much the same manner as health plans, the need under workers' compensation systems to coordinate the health benefits provided with both the indemnity benefits (e.g., lost wages and disability payments) provided under the system and the determination of a worker's ability to return to work raises potential questions about the appropriateness of certain disclosures of medical information. We are continuing to review the need for federal privacy standards in this area and will inform Congress of any recommendations that we have in this area when we complete our review.

We do not recommend that employers as such be controlled by the legislation. But they should be considered health care providers or payers when they actually perform those activities, and obliged to conduct themselves accordingly. (Controls on employers' use of health information so obtained for other purposes is discussed below in **LIMITATIONS ON USE**).

2. COVERED ACTIVITIES

We recommend that health care be defined to include

- any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body;
- any sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; and
- procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

3. COVERED INFORMATION

We recommend that health information include any information, oral or recorded, in any form or medium, including demographic information

- that relates to the past, present, or future physical or mental health or condition of a patient, the provision of health care to a patient, or the past, present, or future payment for the provision of health care to a patient;
- that is received, created, used, or maintained by a health care provider in the ordinary course of business or practice of a profession, or by a health care payer, or received by entities receiving information under the provisions of the legislation without patient authorization; and
- that identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the patient.

We recommend that the legislation cover any information about the patient held by providers and payers for their health care and payment activities. Thus, information that in other settings

would not be health information -- name, identification number, employment status, address, financial data, family size, education, employment history -- should be covered by the protections of the legislation we recommend if held by a health care provider or payer for health care or payment purposes.

The description of identifiability we recommend follows the text of the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (Social Security Act § 1171(6)). We recommend that a legislative definition be no more specific at this time. A precise advance definition is difficult, and there is inadequate basis at this time for recommending one. The only effective formulation now is a test of reasonableness: Information is identifiable if there is a reasonable basis to believe that the information can be used to identify an individual.

No single rule can define what constitutes readily identifiable data. Information is clearly identifiable if it includes a name, social security number or other generally known or readily available identification number, or photograph. Health information will normally be identifiable within providers and payers, and the identifiability question will typically have to be answered when information is to be disclosed outside a provider or payer. Reasonableness may depend on a judgment based on what other information is known to be available to a recipient, and the amount of effort and time that would be needed to achieve a positive identification.

Other legal formulations are not more precise than the HIPAA formulation. The European Union data protection directive, a recent well-debated formulation of privacy rules, uses this test:

an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (Art. 2(a))

The Council of Europe's "Recommendations of the Committee of Ministers to Member States on the Protection of Medical Data" (No. R(97)5 (1997)) states a reasonableness test, but adds an "effort" standard:

....the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower. (Appendix, Art 1.)

The standard we recommend should not be read to mean that information is identifiable if there is a remote chance that somebody might possibly be able to identify a patient from a general description. The Panel on Confidentiality and Data Access of the Committee on National Statistics addressed this issue, and noted that zero-risk requirements for disclosure of statistical records were unrealistic. It recommended a standard that calls for a "reasonably low risk of disclosure of individually identifiable data." (George T. Duncan et al, eds., *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics* 137 (1993)). The

panel recommended that the Office of Management and Budget should continue to coordinate research work on statistical disclosure analysis (at 155-157). This will be especially important as changes in the character and availability of technology alter the quantum of information constituting an identifier. Our recommendations include authority for issuance of guidelines for what levels and amounts of information constitute "identifiable" information, and guidelines for minimum allowable disclosures in particular situations (IMPLEMENTATION, below).

Records disclosed in a form not intended to be individually identifiable should not be used intentionally to identify a person. A person who obtains such information with the intention of identifying individuals should be regarded as having obtained health information under false pretenses (CRIMINAL PENALTIES, below).

Our recommendations do not distinguish among different types of health information based on presumed sensitivity, although we recommend leaving in place State and Federal laws that make that distinction. Our intent at this time is to recommend a meaningful minimum floor of privacy protections in Federal law for all types of health information. At the same time, we recognize that there are arguments for providing additional protection to certain types of health information that people view as particularly sensitive. We can learn from, and build on, States' experience with privacy laws that protect such information, and work with interest groups, privacy advocates, and others to assess how such information is best protected. Such information could be the subject of future Federal action; we look forward to working with the Congress in determining when such protections are appropriate.

7 { We recommend that research in which care is not delivered not be considered "health care," and thus not covered. There are some existing protections for information gathered solely for research, which should continue to apply (RESEARCH, below).

4. SERVICE ORGANIZATIONS

Agents in our bill
We recommend that providers and payers, and those receiving information under the provisions of the legislation without patient authorization, be permitted to engage other organizations, "service organizations," pursuant to contractual arrangements, to carry out functions for them that require use of health information.

We recommend that providers and payers be required to advise their service organizations that their work is subject to the law, whereupon these organizations should become subject to the law.

We recommend that service organizations be obliged to observe the use and disclosure restrictions, and to have a statement of information practices and

to make it available upon request, but not be obliged to provide subject access and correction rights.

Much health information obtained and used by the providers and payers is processed by service organizations engaged by contract. The patient does not have a direct relationship with these organizations and typically does not know of their role in the flow of information.

Physicians and other providers engage companies to code, and to process bills and forward them to the appropriate payer. These companies may in turn deal with others engaged by payers. Between them, yet other companies may process health information by passing it from a provider's clearinghouse to a similar organization engaged by a payer. In some instances, these organizations make substantive or adjudicatory choices affecting the patient on behalf of their principals. In others, they do not, and may not retain the information in ways that permit easy retrieval.

Often there are not clear distinctions among the functions these many processors are performing. As an agent of a payer, a pharmacy benefit management company adjudicates and pays claims, and may manage a formulary. It also provide health care, in conjunction with the pharmacist, in looking for drug interactions -- advising the pharmacist, physician, or patient that a prescribed drug taken in combination with one prescribed earlier may have adverse effects. A payer may engage a pharmacy benefit manager to operate a disease management program to assist patients in managing their illnesses, often chronic conditions such as asthma and diabetes, by education through direct mail and telephone communication to the patient, online communication with physicians and pharmacists, and video materials.

We recommend that everyone in this chain of information handling be covered by the same rules.

Patients must be assured that their privacy protections are not lessened when the providers or payers with which they have established relationships give information to outside service organizations for processing. Thus, service organizations, once advised of the nature of the information they are handling, should be independently bound by the confidentiality restrictions applicable to the principal which engaged them.

They should not use or disclose patient information unless their principals explicitly permit, and the principals should be bound by the legislation in granting such permission. Thus, a service organization should not make independent use of this information unless the provider or payer permits such use, and then only if the legislation permits such use, i.e., with the authorization of the patient, or for a purpose for which the payer or provider could use it or disclose it.

The complexity and multitude of these arrangements, and the typical lack of contact with the patient, make it impractical to impose on service organizations the obligation to provide access and correction rights (discussed below in **PATIENT INSPECTION AND COPYING OF RECORDS** and **PATIENT CORRECTION OF RECORDS**.) However, patients should be

able to exercise these rights by contacting their providers or payers, and providers and payers may by contract require their processors to provide the necessary access and correction. Service organizations should not be required by law to offer patients a statement of the information practices, but they should be required to have such a statement and to make it available upon request.

Processing of information by these organizations is a natural and understandable source of concern. There have been proposals that patients be permitted to forbid the computerization of their records, or otherwise to control directly the flow of information through the payment system. The National Committee on Vital and Health Statistics considered this possibility and had this observation:

The Committee is not sympathetic to the notion that patients should have a choice in the technology used to create, store and transmit health information. This is not a choice that record subjects [have] for records maintained by other third party record keepers such as banks and employers. Requiring health record keepers -- who are spending vast sums on computerization -- to retain parallel paper systems is impractical and costly. It would deny the benefits and savings that the Congress has already determined will result from increased use of modern information technology. Computers are an inevitable part of modern health care and indeed are intrinsic to the actual delivery of hospital care today. Patients must accept this and move on to debate the proper protections for records in a computerized environment. (Health Privacy and Confidentiality Recommendations of the National Committee on Vital and Health Statistics, Approved on June 25, 1997)

Control at this level of detail would be harmful to patients, since the effective and rapid processing of information, often for the benefit of the patient, depends on computerized systems. Our recommendation is for legislation that permits relationships necessary to operate the care and payment system, with common legal controls on all concerned to protect the patient information.

However, should it appear in the future that patient interests are being compromised by contractual arrangements that obscure choices about use and disclosure of information, or that thwart legitimate patient control over information, Congress might want to consider imposing obligations directly on these entities.

In addition to engaging outside organizations to process information about patients, providers and payers will on occasion need to give identifiable information to attorneys, insurers, auditors, and similar special-purpose service organizations. These recipients should be subject to the same use and disclosure restrictions that apply to the information in the hands of the providers and payers.

A similar mechanism, provision for a "qualified service organization," has long been in use under the Federal substance abuse confidentiality statute (Public Health Service Act § 543, 42 U.S.C.

§ 290dd-1). The regulation interpreting that statute permits substance abuse treatment providers to share patient information with outside organizations under agreements similar to the ones we propose here (42 C.F.R. §§ 2.11 (*Qualified service organization*) and 2.12(c)(4)).

5. SERVICE ORGANIZATIONS - GOVERNMENT AGENCIES

We recommend that providers and payers which are Federal, State, or local government agencies be permitted to employ other government agencies, in accord with applicable law, to carry out functions for them that require identifiable health information. The other governmental organizations should be subject to the same disclosure and use restrictions as the covered entity.

This is a governmental counterpart to the previous recommendation. Entities which provide or pay for health care, including government agencies, should be obliged to limit patient health information to the units or organizations actually performing those functions. However, government health providers or payers might on occasion use either outside private organizations (as discussed above) or other parts of their own departments or other departments of government for functions that involve personally-identifiable information, such as central data processing facilities. Likewise, State attorneys general's offices, and the Department of Justice, provide legal services to State and Federal health care facilities and may in the course of that work have access to health information. For such divisions of work within government, existing statutes may govern relationships, and the private contractual model is not directly useable. But the service agencies should be subject to the same use and disclosure restrictions as the covered entity, and thus should not use information about patients obtained in the course of this work for other purposes.

B. BASIC REQUIREMENTS

We recommend that there be a duty not to use or disclose health information except as authorized by the patient, or as explicitly permitted by the legislation.

We recommend that there be no duty to disclose information (except to the patient), and that other laws providing greater protection for health information, or rights for the patient, remain in effect.

1. LIMITATIONS ON USE

We recommend that providers and payers and those receiving information under the provisions of the legislation without patient authorization be permitted to use the health information only for purposes compatible with

and directly related to the purposes for which the information was collected or received, or for purposes for which they would be authorized to disclose the information.

We recommend that legislation constrain the use of information within organizations. Organizations with many purposes and activities do on occasion create or collect information while acting as health care providers or payers. They may also receive information from providers or payers.

The fact that an organizational entity holds information is not a proper basis for its uncontrolled use within the organization. Under the requirement we recommend, entities holding records should have to make distinct and explicit choices about which activities are sufficiently connected with their health activities to warrant the use of identifiable health information. Other uses could be made only with patient authorization, or under provisions of the legislation that permit disclosure without patient authorization.

This requirement should not interfere with normal uses of information in the health care delivery or payment process, but should prevent uses extraneous to health, and may limit some existing uses of health information. We recommend that this be a somewhat more restrictive control than the Federal Privacy Act, which permits disclosure to officers and employees of the agency maintaining the record who have a need for the record in the performance of their duties (5 U.S.C. § 552a(b)(1)).

It is not possible or desirable to set forth in legislation all appropriate internal uses for health information by providers and payers. A general statutory standard is required, and so our recommendation calls for limiting use of health information to purposes compatible with and directly related to the purpose for which the information was collected or received.

For hospitals, for example, the use of health information to provide health care is obviously within the purpose of collection, and providing health care includes a wide variety of activities like management analysis, quality assurance and similar oversight activities, carrying out mandates of law, teaching, training, and research activities. Likewise, a provider or payer should be permitted to use information internally for a purpose for which it could make a disclosure.

This limitation on how patient information is used is especially applicable to organizations that are not primarily health care providers or payers, but that perform those functions, such as employers. This proposal is not intended to cover employers as such. Existing laws (such as the Americans with Disabilities Act of 1990 § 102 (42 U.S.C. § 12112) and the Rehabilitation Act of 1973, (29 U.S.C. § 793) (with regulation at 41 C.F.R. § 60-741.23)) constrain the collection, use and disclosure of health information by employers and should not be disturbed.

But we recommend that employers, when they function as providers or payers, be required to conduct themselves as such under the legislation. Workers have worried that employers get

health information about them, and often their families, in the claims payment process, and may use it to discriminate against them. (Marilyn J. Field and Harold T. Shapiro, eds., *Employment and Health Benefits: A Connection at Risk* at 148 (1993)). This study by the Institute of Medicine recommends explicitly (at 246) that employer access to certain information collected in connection with health benefits be limited through controls similar to those in the Americans with Disabilities Act of 1990.

We recommend just such controls, by regulating how an employer uses information received in the payment process, either as a self-insurer or by processing claims en route to an insurance company. Information should not be used outside of the payment activity. An employer could not use it, for example, to make decisions about promotions or job assignments. Even if employers have information in identifiable form for statistical and analytic operations related to payment, or for oversight of an outside payer, the legislation should forbid its use for anything but these payment-related purposes. Employers should be required to build impermeable barriers between activities that use health information and their other activities.

The same considerations apply to health care delivered by an employer, or on the employer's premises, or by employee assistance programs. The information obtained in rendering these health services should not be used by the employer for purposes outside the purposes for which it was collected, except as authorized by the patient or otherwise allowed by the law.

The examples here are from the employment context; the requirement should be applicable to all who have health information.

2. SAFEGUARDS AGAINST DISCLOSURE

We recommend that providers and payers and those receiving information under the provisions of the legislation without patient authorization be required to maintain reasonable and appropriate administrative, technical, and physical safeguards

- to ensure the integrity and confidentiality of health information; and
- to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information.

We recommend the statutory formulation of a basic obligation of all record holders -- to safeguard the information.

No legislation can effectively specify how to do this, but it can require diligent and attentive choices of security measures. The technology is varied and dynamic, and different types of technology and information call for different types and degrees of security. We recommend that

the legislation require providers and payers to take the appropriate levels and types of protective measures. The legislation should not create an obligation of absolute security. The key words are "reasonable," "appropriate," and "reasonably anticipated," to permit consideration of the degree of risk, the likely consequences of compromise, and the expenditure, financial and other, required to address the risk.

The measures should especially include employee education, clear and certain punishment for misuse, and technical controls on access to information within an organization, since there is evidence that a substantial threat to information is careless or deliberate misuse by those who have authorized access to it in their normal work activities.

A growing body of policy and technical material will help managers in formulating their plans in this regard.

The Office of Management and Budget has promulgated policy establishing a minimum set of controls to be included in Federal automated information security programs (OMB Circular A-130, Management of Federal Information Resources, Appendix III, (February 1996)).

A recent study (commissioned by the National Library of Medicine of the National Institutes of Health and funded by the Library with additional support from the NIH Warren G. Magnuson Clinical Center and the Massachusetts Health Data Consortium), identifies best practices in social and technical mechanisms for protecting privacy and maintaining security that are currently used in information systems for health care. (National Research Council, Computer Science and Telecommunications Board, *For the Record: Protecting Electronic Health Information* (1997)).

The Health Insurance Portability and Accountability Act of 1996 requires the Secretary of Health and Human Services to develop standards for electronic transmission of financial and administrative information about health transactions, including security standards. Most of these standards will be published for initial comment this year.

The Center for Democracy and Technology has produced *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality* (1996), a guide to help designers of electronic health information systems to identify and deal with confidentiality issues.

The Computer-based Patient Record Institute (CPRI) has produced a series of publications with guidance on security policies for computer-based patient records. (*Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records* (January 1996), *Guidelines for Information Security Education Programs* (June 1995), *Guidelines for Managing Information Security Programs* (January 1996), *Sample Confidentiality Statements and Agreements* (May 1996), and *Security Features for Computer-based Patient Record Systems* (September 1996)).

3. MINIMUM DISCLOSURE

We recommend that all uses and disclosures be restricted, to the extent practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed.

This recommendation is for an obligation to design systems to limit the amount of information that is disclosed to the minimum necessary for the intended purpose.

Any judgment about what is practicable, and what is minimum, must take into account the technical capabilities of record systems and the costs of limiting uses and disclosures. It is likely to be easier to limit disclosure when disclosing computerized records than when providing access to paper records. Technological mechanisms to limit the amount of information available for a particular purpose, and make information available without identifiers, are an important contribution of computerization to personal privacy. For example, limited fields of information can be disclosed, and identifiers can be stripped. As a practical matter, sorting through paper records to ensure that only the minimum amount is disclosed will be expensive and time-consuming and can risk compromising the integrity of the record, and these factors relate to practicability.

As technologies develop, it will become easier and cheaper to provide minimum information and to limit disclosure. We recommend that a Federal agency be authorized to issue guidelines for what levels and amounts of information constitute "identifiable" information, and guidelines for minimum allowable disclosures in particular situations.

Recent studies have emphasized the value of privacy-enhancing technologies (PETS) in accomplishing necessary transactions with a minimum of identifying information. The Dutch Data Protection Authority and the Information and Privacy Commissioner for the Province of Ontario, Canada, both governmental privacy protection entities, recently collaborated in producing a report exploring privacy technologies that permit transactions to be conducted anonymously. (Information and Privacy Commissioner/Ontario, Canada, and Registratiekamer, the Netherlands, *Privacy-Enhancing Technologies: The Path to Anonymity* (1995)).

The provision we recommend should not be a basis for automatic withholding of records in situations where the requester is best positioned to determine what information is necessary, such as oversight and public health investigations.

C. PATIENT AWARENESS AND CONTROL

1. EXPLANATION OF INFORMATION PRACTICES

We recommend that providers and payers, and those receiving information under the provisions of the legislation without patient authorization, be required to prepare a written notice to inform patients of their information practices and of the patients' rights regarding the health information.

We recommend that the explanation be required to provide information on whatever rights the patient has with respect to information, including, if applicable

- the uses and disclosures of information authorized under the legislation and intended by the holder, as well the protections available;
- the right of the patient to prevent or limit disclosure in whatever circumstances that right exists;
- the right to inspect and copy information and to seek amendments;
- the procedures for authorizing disclosure of information and for revoking disclosure authorizations;
- the procedures for the exercise of rights under the legislation, and the procedures, if any, for complaint, redress, or appeal; and
- the fact that service organizations and those receiving information under the provisions of the legislation without patient authorization have explanations of information practices which are available upon request.

We recommend that providers and payers be required to give patients this explanation, or at least advise patients affirmatively of its availability and provide a copy upon request.

We recommend that service organizations and those receiving information under the provisions of the legislation without patient authorization be required to develop explanations of information practices meeting the same standards, and to provide a copy to patients upon request.

An informed citizenry is essential to protection of privacy. The basic structures for protection of health information should include requirements that patients be told what is being done with information about them, and what their rights are.

The Privacy Working Group of the President's Information Infrastructure Task Force formulated personal privacy principles (*Principles for Providing and Using Personal Information* (June 1995)), and three of them point to the centrality of public information and education:

II.B. Notice Principle. Information users who collect personal information directly from the individual should provide adequate, relevant information about:

1. Why they are collecting the information;
2. What the information is expected to be used for;
3. What steps will be taken to protect its confidentiality, integrity, and quality;
4. The consequences of providing or withholding information; and
5. Any rights of redress.

II.E. Education Principle. Information users should educate themselves and the public about how information privacy can be maintained.

III.A. Awareness Principle. Individuals should obtain adequate, relevant information about:

1. Why the information is being collected;
2. What the information is expected to be used for;
3. What steps will be taken to protect its confidentiality, integrity, and quality;
4. The consequences of providing or withholding information; and
5. Any rights of redress.

Likewise, the National Information Infrastructure Advisory Council (a public advisory committee to the President's Information Infrastructure Task Force) issued a statement, *Common Ground: Fundamental Principles for the National Information Infrastructure* (March 1995), which includes the following among its privacy and security principles:

10. Collectors and users of personally identifiable information on the NII should provide timely and effective notice of their privacy and related security practices.

11. Public education about the NII and its potential effect on individual privacy is critical to the success of the NII and should be provided.

The reasoning behind these principles emphasized that the public should be aware of uses and transfer of information that may not be clear or obvious. Health information is transmitted and used by a large number of agencies and institutions, and patients should know at least in a

general way where it is going, how they can make corrections, and how to find out more information.

*Informed
Consent* The explanation is of special importance in view of our recommendation below (HEALTH CARE AND PAYMENT) that disclosures of health information for health care and for payment be permitted without patient authorization, but that patients be permitted to object to particular disclosures for these purposes. The explanation of the patient's right in this regard is an integral element (together with direct legal controls on use of information by providers and payers) of this more realistic and informed patient control of information that we offer to replace the consent processes under which patients now permit their records to be passed around.

The Privacy Act of 1974 requires that Federal agencies advise the subjects of Federal records of their intended uses (5 U.S.C. § 552a(e)(3)). Cable television subscribers are entitled, under the Cable Communications Policy Act of 1984, to an annual notice of the cable company's information practices (47 U.S.C. § 551(a)). The recommended requirement would bring these salutary practices to health information.

All organizations should be required to have statements to inform patients, if they request it, of how they use health information, and what the rights of the patients are. The health care providers and payers, which have direct relationships with patients, should make this explanation available in an affirmative fashion, for example, at health care facilities, or with written material sent by mail to subscribers to health insurance plans. We recommend that the legislation require a written explanation that can be retained by the patient, so that patients can examine the policies and become aware of their rights at their leisure (when not under the anxiety sometimes attendant to receiving health care) and consult others as necessary. At the same time, we do not believe that it is desirable to prescribe in legislation the details of how the notice should be given.

Federal agencies could incorporate in the explanation proposed here the notice of information practices required by the Privacy Act.

Organizations that do not have direct contact with patients should also be required to prepare such an explanation and to make it available upon request.

2. PATIENT INSPECTION AND COPYING OF RECORDS

We recommend that patients be allowed to inspect and copy health information about them held by providers and payers. We recommend that patients be allowed to inspect and copy health information held by public health authorities, and by oversight agencies in any situation in which an oversight agency has made an adverse decision about the rights, benefits, or privileges of the patient.

~~We recommend that those holding health information be permitted to deny~~
patient inspection of particular information under any of these
circumstances:

- the information is about another person (other than a health care provider) and the holder determines that patient inspection would cause sufficient harm to another individual to warrant withholding.
- inspection could be reasonably likely to endanger the life or physical safety of the patient or anyone else.
- the information includes information obtained under a promise of confidentiality (from someone other than a health care provider), and inspection could reasonably reveal the source.
- the information is held by an entity that has received it under the health oversight provisions of the legislation, and access by the patient could be reasonably likely to impede an ongoing oversight or law enforcement activity.
- the information is collected in the course of a clinical trial, the trial is in progress, an institutional review board has approved the denial of access, and the patient has agreed to the denial of access when consenting to participate.
- the information is compiled principally in anticipation of, or for use in, a legal proceeding.

We recommend that providers and payers be permitted to deny inspection if the information is used solely for internal management purposes and is not used in treating the patient or making any administrative determination about the patient, or if it duplicates information available for inspection by the patient.

We recommend, in instances where a patient is to be denied inspection, that the holder of the record be required to make available to the patient, to the maximum extent possible, any portion of the health information which is not allowed to be denied to the patient under the standards above.

We recommend that providers and payers be permitted to charge a reasonable, cost-based fee for inspection and copying a record.

We recommend that entities obliged to provide inspection rights be required to make a decision on patient inspection within 30 days of a request, and that if they deny inspection rights they be required to give the patient a written statement of the reason.

We recommend that existing rights of subject access and correction under the Privacy Act of 1974 not be diminished.

The ability to see one's own record is central to effective control of information and is a basic fair information practice. A patient's decision whether to disclose a record may depend on what the record says, and so access to the record is integral to making an informed choice to disclose information.

The "Code of Fair Information Practice" recommended in 1973 by the Secretary's Advisory Committee on Automated Personal Data Systems includes as one of its five basic principles:

There must be a way for an individual to find out what information about him is in a record and how it is used.

(U.S. Department of Health and Human Services, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 41 (1973)).

The Privacy Protection Study Commission recommended that this right be available. (*Personal Privacy in an Information Society* 299 (1977)). A right to see one's record is available by law in 31 States (described in Public Citizen Health Research Group, *Medical Records: Getting Yours* (1995)), and has been a right (with very limited exceptions) in Federal health record systems since the Privacy Act of 1974 (5 U.S.C. § 552a(d)).

The exceptions that we recommend provide for the limited situations in which, in the judgment of health professionals, access to the record by the patient would cause grave harm, or, in the case of oversight activities, would endanger the oversight activity, or in the case of clinical trials, would endanger a trial.

There should be no obligation to employ the exceptions. In general, patients should be able to see and copy their records, but there should be a provision to permit health professionals to exercise their judgment to withhold information in the rare instances where that is appropriate. Further, the record holder should be able to deny access only to the portion of the record that falls within the stated exceptions. The record holder should redact the portions allowed to be denied, and should give the patient the rest of the information.

There need be no obligation to let patients see information used solely for internal management purposes, which is a duplicate of the basic patient record (e.g., a back-up copy), or which is gathered for litigation.

Some clinical trials will involve health care and thus will be covered by the law, and the usual right to see one's record raises a special issue in these cases. We believe that a right to see one's own record, properly managed, need not impair research.

Subjects in clinical trials are often, by design of the research, unaware of the identity of the medication they are taking, or of other elements of their record. The research design precludes their seeing their own records and continuing in the trial. Further, patient access during the trial could endanger the entire trial.

Thus, we recommend that it be clear that a patient can waive the normal right to inspect information while the trial is in progress, regardless of the length of the trial. This waiver would be an element of the patient's consent to participate in the trial. The institutional review board should have to approve it, and the patient should be told clearly of this condition. The subject should have the usual right to see the record after the trial is completed.

Some entities other than providers and payers should be obliged to provide patient access (and the related correction rights, described below). Public health agencies may be able to take actions to affect the lives of the patients. Some health oversight agencies can make operational choices that affect the patient, such as denial of payment, and it is essential that patients be able to see records held by these agencies, after a decision adverse to the patient is taken. Under current law, such disclosure is already required, and through adversary proceedings, patients can challenge incorrect information which served as the basis for the adverse decision.

In other instances (e.g., an accreditation study of a hospital by the Joint Committee on Accreditation of Health Care Organizations) no individual patient interest is at stake in the oversight activity, and access is less significant.

However, the right recommended here is not simply a right to fair procedure in an administrative transaction or criminal or civil legal action (which may be provided in any case by other law); it is a freestanding fair information practice right to see one's record at a time of one's choosing regardless of actual use in a proceeding or for decision making. It should be available unless there is a danger that patient access would impede the investigation. We recommend that any procedures established to implement these provisions not be unduly burdensome on law enforcement or oversight agencies.

We do not recommend that researchers who receive information under the provisions of the legislation without patient authorization be obliged to permit patient access. In most instances, they have no direct contact with patients, and under our recommendations would be prohibited from using such information against a patient.

The section on **SERVICE ORGANIZATIONS**, above, addresses the rights of patients to see information held by service organizations operating on behalf of entities that are obliged to give patients access to their records.

3. PATIENT CORRECTION OF RECORDS

We recommend that patients be permitted to seek correction or amendment of health information about them held by any entity obliged to permit patients to inspect health information about them.

We recommend that these conditions govern responses to such requests:

- if the entity makes the requested change, it must make reasonable efforts to inform others who have received the incorrect information about the change,
 - who are identified by the patient; or
 - who the entity knows have received the information, when it is reasonably foreseeable that the incorrect information may have an adverse impact on the recipient or patient.
- if the entity makes the requested change, it must make reasonable efforts to inform known sources of incorrect information.
- if an entity denies a request, it should inform the patient of the reasons for the denial and of any procedures for further review. The burden of proving that information needs to be amended or corrected should fall on the patient, and the legislation should not require a process for further review.
- if a patient's request is denied, the patient should have the right to file a concise statement with the requested correction and the patient's reasons for disagreeing with the refusal. This statement should be included in any subsequent disclosure of the disputed portion of the information about the patient. The holder may include a concise statement of its reasons for not making the requested change.

This recommendation is intended to ensure basic fairness with respect to accuracy of information. It follows the pattern established by the Privacy Act of 1974 for Federal agencies (5 U.S.C. § 552a(d)(2)). It is not intended to interfere with medical practice, or modify standard record-keeping practices.

Reasonable attempts at notification of others should prevent the perpetuation and further transmission of erroneous information. The legislation should explicitly state a test of

reasonableness in this regard, so that the vigor of the effort required is proportional to the importance of the information and the degree of hazard in disseminating incorrect information.

We recommend that it be clear that this provision is not intended to provide a procedure for substantive review of decisions such as coverage determinations by payers. It is intended to deal with the content of records, not the underlying truth or correctness of the events recounted in them. Attempts under the Privacy Act of 1974 to use the Act's correction mechanism as a basis for collateral attacks on agency determinations have generally been rejected by the courts. We intend the result to be the same here.

It is the standard practice of medical record keepers not to expunge any information in a treatment record. The usual procedure is to mark incorrect information and to add the correct information. Even if information is wrong, it is essential to the purpose of the medical record that the record reflect the information available when treatment decisions were made. We recommend no change in these practices, and there should be no requirement that information be erased or deleted. A record should be considered corrected or amended if incorrect information is marked as such, and the correct information added.

4. DISCLOSURE HISTORY

We recommend that providers and payers, and those receiving information under the provisions of the legislation without patient authorization, be required to retain a history of all disclosures of health information made for treatment, payment, research, oversight, public health, emergencies, to State data systems, for law enforcement, in judicial proceedings, and with the authorization of the patient.

We recommend that the record include the date and purpose of the disclosure; the name and address of the person to whom the disclosure was made or the location to which the disclosure was made; and where practicable, a description of the information disclosed.

We recommend that patients be permitted to see this record, except in the case of disclosures to and by health oversight agencies and to law enforcement agencies where access by the patient could be reasonably likely to impede those activities.

We recommend that the disclosure history be retained for the life of the record to which it relates.

We recommend that there be no obligation on service organizations to retain a record of disclosures in the course of treatment and payment transactions.

What is the point of keeping disclosure records if patients can't view?

Patients ought to know who has seen information about them. This basic right was recommended by the Privacy Protection Study Commission (*Personal Privacy in an Information Society* 316 (1977)), and is available, with limited exceptions, under the Privacy Act of 1974 (5 U.S.C. § 552a(c)). The ability to see who has seen one's record is a form of control on disclosure. In a health facility where employees who receive care at the facility can easily check who has accessed their records, they often do check, and staff at the facility see this as an important confidentiality control (National Research Council, Computer Science and Telecommunications Board, *For the Record: Protecting Electronic Health Information* 98 (1977)).

Our recommendation does not envision that the legislation specify any particular form for retention of this history, as long as the inquiring patient can find out where his or her information went. Health facilities may choose to keep the disclosure history in a patient file, in a separate log, or in any other way, as long as it is possible to identify or accurately reconstruct the disclosures.

Our recommendations call for an exception to the right of patient access when access could be reasonably likely to impede oversight or law enforcement activities. We recommend that any procedures to implement these provisions not be unduly burdensome on oversight or law enforcement agencies.

No accounting should be required for disclosures made under the next-of-kin and directory information provisions (described below).

D. DISCLOSURES AUTHORIZED BY THE PATIENT

1. DISCLOSURE WITH PATIENT AUTHORIZATION: AUTHORIZATION CONTENT

We recommend that providers and payers, and those receiving information under the provisions of the legislation without patient authorization, be permitted to disclose information pursuant to the authorization of a patient under the following conditions:

- the authorization is in writing, is dated, and is signed or otherwise authenticated;
- the authorization states an expiration date, or event, and is received by that date or event;
- the authorization specifies the information to be disclosed;
- the authorization specifies the entity or entities which are to disclose the information;

- the authorization specifies the person or persons to receive the information;
- the authorization states that the patient has received a statement of the intended use of the information by the recipient; and
- the authorization is not on the same form on which a patient consents to health care, and states that treatment, coverage, and payment are not conditioned on the patient's authorization to disclose, unless the disclosure is necessary for treatment, coverage, or payment.

We recommend that a person who requests a patient to authorize disclosure of health information be required to give the patient a copy of the authorization.

We recommend that a patient be permitted to revoke an authorization to disclose information except to the extent that action has been taken in reliance on the authorization.

We recommend that entities disclosing information pursuant to an authorization be required to retain a copy of the authorization, and a record of the disclosure.

The ability to control use and disclosure of information is central to fair information practices, and we recommend requirements to ensure that the patient understands the nature of the disclosure being authorized, and to ensure that there is adequate specificity to the patient's authorization, and to ensure that authorizations do not become general permissions for unrelated disclosures.

The required signature may be an electronic authentication.

To assist in preparing these authorizations, the Federal agencies should be authorized to publish model authorization forms and model statements of intended uses (see below, IMPLEMENTATION).

2. DISCLOSURE WITH PATIENT AUTHORIZATION: EXPLANATION, AGREEMENT, AND REMEDY

We recommend that a person who requests a patient to authorize disclosure of health information be required to provide a statement for retention by the patient, not on the same form as the authorization, specifying the purposes

for which the information is sought and the uses and disclosures to be made of it.

We recommend that use or disclosure of the health information inconsistent with the statement be the basis for a civil action for damages.

This recommendation is intended to provide patient control in the many situations in which patients authorize others to receive health information about themselves. It addresses information that moves beyond the direct scope of the law we recommend.

These disclosures are made for many reasons. Applicants for life or disability insurance authorize providers to disclose existing information about themselves, and are informed by the insurer how the information will be used, including, for example, for reports to the Medical Information Bureau, a clearing house of information about life and disability insurance applicants to detect fraudulent applications.

Claimants in liability situations authorize their providers to send information to liability insurers to show the extent of their injuries. In case which move to litigation, a plaintiff will typically authorize an attorney to receive medical records and transmit them to medical consultants for review, and then to the defendant's insurer, to show the extent of the plaintiff's injury.

Patients may authorize disclosure of health information when receiving other services, such as social services. Disability determinations in the disability program under the Social Security Act are dependent on the patient's offering evidence of his or her health condition. People may authorize disclosure of their information for suitability investigations by government agencies, or for employment or assignment determinations.

Legislation cannot address all the possible uses of health information by the great variety of persons and organizations that may receive it pursuant to patient authorization. Nonetheless, patients properly expect fair treatment of this information, and should be able to enforce that expectation. This information, obtained as it is from the health care setting, retains its sensitivity, and should be protected in a legally enforceable way. Collection of damages for use inconsistent with the stated purpose is the recommended enforcement mechanism.

This recommendation provides that protection by permitting the patient to enforce the agreement the patient and the recipient make.

The recipient may choose to promise essentially no confidential treatment, or may choose to specify, in general or in particular, how the information may be used. In some instances, other law will govern how the information may be further used (as in some collections of health information by government agencies), and that law would define the recipient's promises to the patient. The patient may be able to take these promises into account in deciding whether to disclose information in a particular instance.

To assist in developing such agreements, the Federal agencies should be authorized to prepare model authorization forms and model statements of intended uses (see below, **IMPLEMENTATION**).

This recommendation would implement one of the *Principles for Providing and Using Personal Information* (discussed above in **EXPLANATION OF INFORMATION PRACTICES**), formulated by the Privacy Working Group of the President's Information Infrastructure Task Force:

III.C. Redress Principle

Individuals should, as appropriate, have a means of redress if harmed by an improper disclosure or use of personal information.

The President's statement on the Global Information Infrastructure, *A Framework for Global Electronic Commerce* (June 1997), in its discussion of privacy, reiterates this point:

Under these principles, consumers are entitled to redress if they are harmed by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information.

3. **DISCLOSURE WITH PATIENT AUTHORIZATION: PROHIBITION ON REQUIREMENTS TO AUTHORIZE DISCLOSURE**

We recommend that providers be forbidden to condition treatment on the patient's authorization to disclose health information, unless the disclosure is necessary for a health care or payment purpose.

We recommend that payers be forbidden to condition coverage or payment on the patient's authorization to disclose health information, unless the disclosure is necessary for a health care or payment purpose.

We recommend that providers and payers be required, when requesting an authorization to disclose information for purposes other than health care or payment, to advise patients that treatment, coverage, and payment are not conditioned on the patient's authorization to disclose.

We recommend this requirement so that providers and payers cannot require patients to authorize disclosure of health information as a condition of treatment, coverage, or payment unless the disclosure is actually necessary for those purposes. Such demands could nullify the legislation's controls on disclosure of information. If needed benefits or services are not available unless the patient consents to disclose information, patients could be unfairly compelled to permit disclosures beyond those permitted by the legislation.

A patient seeking care or payment should be informed that he or she can resist a request for an authorization. It is important that the authorization clearly state that the patient will receive the same treatment, coverage, or payment, whether or not the authorization is signed.

(DISCLOSURE WITH PATIENT AUTHORIZATION: AUTHORIZATION CONTENT, above).

This requirement should not interfere with health care or the normal operation of the payment system. Patients may properly be required to make available information necessary to treat them, or for reimbursement. Likewise, where such requests are not forbidden by other law, patients could be asked to disclose information about past health history for underwriting purposes. Patients could be asked to authorize disclosure for purposes other than health care or payment, like marketing, as long as treatment, coverage or payment is available whether or not the patient authorizes the disclosure.

This recommendation is not intended to prevent researchers from requiring subjects to agree to disclosures necessary for participation in a clinical trial. Research subjects are often asked to consent to disclosure of their past health history, as well as to permit information generated in the trial to be reviewed by sponsoring and oversight agencies. These disclosures are integral to the operation of clinical trials, and the legislation should permit such conditions.

E. OTHER DISCLOSURES

1. HEALTH CARE AND PAYMENT

We recommend that providers and payers and those receiving information under the provisions of the legislation without patient authorization be permitted to disclose health information without patient authorization to provide health care to any patient, and for payment, but that patients be permitted to restrict disclosures of particular information or disclosures to particular persons.

We recommend that the traditional control on use and disclosure of information, the patient's written authorization, be replaced by comprehensive statutory controls on all who get health information for health care and payment purposes.

The reality of the present authorization process is that the patient has little actual control of information. The approach we recommend would replace the often ritualistic authorization with direct statutory controls and a realistic and effective opportunity for patient intervention in instances where the patient finds it truly necessary.

Disclosures for health care are made routinely now. A requirement for a signed paper for a routine referral can impair care by delaying consultation and referral. For example, a physician

may decide, from review of test results after the patient has left the office, to refer the patient for consultation; the patient should not have to journey to the office again to sign a form before the physician can discuss the case with the consulting specialist. The provider should not be constrained in deciding whom to consult unless the patient has specifically indicated a sensitivity to such consultations.

Some existing State health confidentiality laws permit disclosures without consent to other health care providers treating the patient, and the Uniform Health-Care Information Act permits disclosure "to a person who is providing health-care to the patient" (9 Part I, U.L.A. 475, § 2-104 (1988 and Supp. 1996)).

For payment, existing authorizations are often forms that have little meaning to the patient, and that the patient must sign if reimbursement is to be obtained. This process should be replaced by one in which information flows easily and without unnecessary barriers when necessary for payment, while protected by direct legal obligations on providers and payers. Changes in insurance carriers, for example, should not require multiple authorizations. A failure to obtain an authorization should not prevent a health care provider from billing payers who might not be precisely identified when treatment is rendered. In addition, information moves from provider to payer through a chain of processing entities (see **SERVICE ORGANIZATIONS**, above) whose precise identity may not be known to the provider in contact with the patient. A true, fully enforced, authorization requirement for each of these transfers of information would bring the health care payment system to a halt.

The traditional goals of the authorization process are important ones, and we must have strong and realistic ways of meeting those goals. It is our view that stringent statutory protections on information held by providers and payers, and an opportunity for patients to object to particular disclosures (an "opt-out"), can fulfill these goals more effectively than the authorization formula. The explanation of information practices that providers and payers would have to provide should specifically note the patient's opportunity to object to particular disclosures.

The opportunity to object to a particular disclosure is a more realistic and effective form of control than routine signature of an authorization form, and exactly for that reason it may require attention from providers in responding to patient wishes. In turn, patients will have to exercise care and judgment in using it. In the treatment context, some elements of medical history are irrelevant to present treatment; and patients may reasonably want them concealed. A patient's sexually-transmitted disease at the age of 22 need not be announced to all who are treating an athletic injury when the patient is 44.

But current medical history, especially medications, and some past medical history, are very much relevant to present treatment, and the patient cannot withhold this information from subsequent providers without grave risk. There are dangers in making treatment decisions based on incomplete information, and providers may properly decline to treat patients without full understanding of their medical history. Legislation should not prevent physicians from

conditioning treatment on having that history. Thus, if the patient chooses to restrict disclosure for treatment, the patient and the concerned providers would have to negotiate the patient's actual control in light of the need for the history in treating the patient.

Likewise, disclosure to a payer is necessary for reimbursement. To the extent that the patient does not want information disclosed to an insurer or other payer, the patient must address the financial aspects of treatment in some other way.

We recommend that the legislation be written to allow physicians to use any patient's record, not just the record of the patient being treated, to accommodate the practice in which a physician who is treating a patient with a rare disease may examine the records of other hospital patients with the same disease. Likewise, physicians may consult the records of several people in the same family or living in the same household to assist in diagnosis of conditions that may be contagious or that may arise from a common environmental factor.

2. HEALTH OVERSIGHT

We recommend that providers and payers and those receiving information for health oversight without patient authorization under the provisions of the legislation be permitted to disclose health information without patient authorization, if such disclosures are authorized by other law and any requirements of other law have been met, for oversight of the health care system, including

- any assessment, evaluation, determination, or investigation relating to the licensing, accreditation, or certification of health care providers; and
- any audit, assessment, evaluation, determination, or investigation relating to the effectiveness of, compliance with, or applicability of, legal, fiscal, medical, or scientific standards or aspects of performance related to health care or payment, including claims for benefits based on health status, claims of eligibility for programs that produce eligibility for health benefits, and claims for other benefits in programs conducted or funded by governments.

We recommend that public agencies, as well as other entities acting on behalf of public agencies, acting pursuant to a requirement of a public agency, or carrying out activities under a State or Federal statute regulating assessment, evaluation, determination, or investigation with respect to health care, be eligible for this access.

We recommend that standard-setting organizations with which a provider or payer has a contract providing for review of the covered entity's activities be eligible for this access.

We recommend that those receiving information under the provisions of the legislation without patient authorization for research and public health be permitted to disclose health information for oversight of the particular research or public health activity holding the information, and that no use of the information against the patient be permitted except for wrongdoing in connection with the research or public health activity.

We recommend that public agencies receiving information under this provision be permitted to disclose health information in accord with applicable law.

We recommend that other entities receiving information under this provision not be permitted to disclose health information except for oversight purposes.

We recommend that these disclosures be permitted so that there can be effective oversight of health care activities. The types of oversight organizations and activities are many, and range from traditional law enforcement agencies, to government agencies investigating or paying for health care, to the professional licensure and discipline system, to regulators like insurance commissioners, and to accreditation, standard-setting, and quality review organizations and activities.

These activities occur under a myriad of circumstances, including pursuant to complaints about criminal behavior, as part of professional disciplinary proceedings, and pursuant to contract by facilities which wish accreditation and engage organizations to review their activities.

These activities may be performed by a public agency, or by another organization acting on behalf of a public agency, pursuant to a requirement of a public agency, or carrying out activities under a State or Federal statute requiring or otherwise providing for the assessment, evaluation, determination, or investigation. The standard-setting organizations perform their functions pursuant to contract with the institutions they are examining and accrediting.

The common features among these activities are these:

All, at some point in their operations, need access to individually-identifiable records.

Their effectiveness depends on access being controlled by the oversight entity, not the holder of the information, whose behavior and activities are under examination.

The oversight activity is required because of the large volume of fraud and abuse in the health care system. It necessitates a substantial enforcement apparatus, including conventional law

enforcement agencies (such as the Federal Bureau of Investigation, and State and local police departments), and specialized agencies (such as the Inspectors General of the Department of Health and Human Services, the Office of Personnel Management, and the Department of Labor, and State Medicaid fraud control units.) The General Accounting Office has estimated health care losses due to fraud and abuse as approximately 10 percent of outlays.

Some of the activities investigated by the Office of Inspector General of the Department of Health and Human Services display the scope of the issue, and suggest how records are needed in the investigation:

- Billing of Medicare and Medicaid by nursing homes for unnecessary services and services which were not provided at all (OIG Special Fraud Alert, "Fraud and Abuse in the Provision of Services in Nursing Facilities" (61 Fed. Reg. 30623-30625 (1996)), including:

A physician billing \$350,000 over a 2-year period for comprehensive physical examinations of residents without seeing a single resident, and falsifying medical records to indicate that the services were rendered.

A psychotherapist manipulating Medicare billing codes to charge for 3 hours of therapy for nursing home residents when in fact he spent only a few minutes with each resident.

A speech specialist preparing documentation overstating time spent on each session, claiming to spend 20 hours with residents every day, and submitting some claims for residents he had never seen, and some who were dead.

- Billing of Medicare and Medicaid for services by home health agencies that were not provided, or provided by untrained personnel, or otherwise in violation of the rules governing reimbursement of home health services (OIG Special Fraud Alert, "Home Health Fraud, and Fraud and Abuse in the Provision of Medical Supplies to Nursing Facilities" (60 Fed. Reg. 40847-4085 (1995)), including:

Billing Medicare for 123 home health visits to a patient who never received a single visit, and submitting claims for beneficiaries who were in an acute care hospital during the period the agency claimed to have provided home visits.

Billing for a home health aide provided to a beneficiary who was not housebound, and actually very mobile.

Claiming nearly \$26 million during one year in visits that were not made, visits to patients who were not homebound, and visits not authorized by a physician, all

supported by forging beneficiary signatures on visit logs and physician signatures on plans of care.

Review of patient records was essential to the inquiries that identified these abuses. Some oversight activities, such as audits and evaluations, are done without direct access to identifiable patient information, since these inquiries take the form of a statistical inquiry to determine, for example, the rate at which a certain procedure is performed in a hospital or to calculate the average cost of a particular procedure. Computerized techniques make this possible without direct access to identifiers, and it is the practice of oversight agencies to do as much inquiry as possible without identified information.

But there are many instances in which identifiers are needed. Even in a statistical inquiry of the type just described, in a paper environment individual patient charts must be examined, and the patient's name would be disclosed because it would be on each page of the chart.

Other inquiries require review of individual medical records, to identify individual instances of the anomalies in treatment or billing patterns detected in statistical analysis. Billing abuses of the type cataloged above are detected by cross-checking the records of individual patients, to see the medical documentation in support of a service. The oversight agency reviews identifiable records to verify that it is comparing the same treatment history. Once an offense is identified and is to be prosecuted, a complete and intact record is required for evidentiary purposes, and due process requires that persons subject to sanction or prosecution have access to the precise factual basis for those actions.

This recommendation is meant to permit disclosure of health information for inquiries that may not be solely about the actual delivery of health care. The definition of health care and payment encompasses "claims for benefits based on health, and claims of eligibility for programs that produce eligibility for health benefits and claims for other benefits in programs conducted or funded by governments." Fraudulent schemes sometimes involve several government programs, such as public assistance, food stamps, and disability programs, as well as health payment programs like Medicaid. Law enforcement officials work in teams to examine the common patterns in these activities, and we intend to permit, for example, the use of information about Medicaid beneficiaries in such investigations. Programs such as workers' compensation also involve review of health records to determine whether program requirements have been met.

Patient records are needed for other inquiries relating to quality of care, and the rights of patients. The Peer Review Organizations authorized under title XI, part B of the Social Security Act (42 U.S.C. §§ 1320c et seq.) review the quality of care provided to Medicare beneficiaries. The Protection and Advocacy for Mentally Ill Individuals Act of 1986 (42 U.S.C. § 10801 et seq.) authorizes grants for State programs to investigate abuse and neglect of individuals with mental illness, and authorizes access to patient records for this purpose (§ 105(a)(4), 42 U.S.C. § 10805(a)(4)). State insurance regulatory agencies examine the records of insurance companies. The Department of Labor reviews plans under the Employment Retirement Income Security Act

of 1974 (ERISA) (29 U.S.C. § 1134). State professional licensure agencies examine the records of health professionals, and may use evidence in them in taking action against the professionals. In the case of research, Federal reviewers may examine records to evaluate compliance with the regulation for protection of research subjects (45 C.F.R. part 46, and 21 C.F.R. parts 50 and 56). The Nuclear Regulatory Commission reviews records to determine medical licensees' compliance with its regulations.

This recommendation does not propose any new judicial process prior to disclosure. The legislation we recommend should permit access to records without compulsory process where that access is otherwise allowed. However, it should not abrogate or modify other statutory requirements for judicial determinations or other procedural safeguards, or permit disclosures forbidden by other law. It should not abrogate or modify other legal restrictions on redisclosure of information, such as the requirement for court review for disclosure for purposes unrelated to health care of information obtained under the Attorney General's investigative demand authority in section 3486 of title 18 of the U.S. Code, added by the Health Insurance Portability and Accountability Act of 1996, § 248. We also recommend that the legislation make obtaining health information under false pretenses be a Federal felony.

Many investigative agencies have and use compulsory process authority. Inspectors General have it under the Inspector General Act of 1978 (5 U.S.C. App. 3, § 6(a)(4) (1988)). The Attorney General has a new investigative demand authority, mentioned just above, providing authority to examine any medical records in investigating health fraud, with power to invoke the aid of any court in enforcing the demand. In these cases, the statutes under which investigative authorities operate determine the procedure surrounding the demand.

Thus, even if compulsory process is used for an oversight investigation, we recommend that there be no requirement for judicial consideration of the type required in the civil litigation situations described below under **JUDICIAL PROCEEDINGS AND ADMINISTRATIVE PROCEEDINGS: PATIENT AS PARTY** and **JUDICIAL PROCEEDINGS: OTHER**.

3. PUBLIC HEALTH

We recommend that providers and payers and those receiving information under the provisions of the legislation without patient authorization be permitted to disclose health information without patient authorization, for public health purposes to

- a legally constituted public health authority for disease or injury reporting, public health surveillance, or public health investigation or intervention;

- anyone authorized to receive the information to comply with requirements or direction of a public health authority; or
- an individual authorized by law to be notified in a public health intervention.

We recommend that a public health authority be defined as an authority of the United States, a State, a political subdivision of a State, or an Indian tribe, that is formally responsible for public health matters as part of its official mandate.

We recommend that further disclosure by a recipient be limited to health care, public health, research, and oversight of the particular public health activity, except that no restrictions should apply to an individual who is notified in a public health intervention.

Numerous important public health activities use identifiable information about patients. Disclosure and use of information for those purposes, under careful controls to protect the patients, contributes to an important social benefit.

Traditional public health surveillance, investigation, and intervention with respect to communicable disease continues to be important. Infectious disease is still a serious threat to health. In a report on this topic the Centers for Disease Control and Prevention offer as a major objective the expansion and coordination of surveillance systems for the early detection, tracking, and evaluation of emerging infections in the United States. The report states that "[s]urveillance is the single most important tool for identifying infectious diseases that are emerging, are causing serious public health problems, or are diminishing in importance." (Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, *Addressing Emerging Infectious Disease Threats: A Prevention Strategy for the United States* 12 (1994)).

These well-known activities have been supplemented by carefully-designed and valuable assessment activities to collect information about other health conditions and injuries. Assessment activities (e.g., assessing the health needs of the community) embody several core public health practices that all communities need to perform (Michael A. Stoto et al., eds., *Healthy Communities: New Partnerships in the Future of Public Health* (1996)).

Disclosures to facilitate these activities, including both reporting requirements imposed by statute and other collections of data based on more general authority, should be allowed. In all States, certain conditions are required to be reported to public health authorities, but the recommendation permits disclosure without an explicit statutory command to report an item of information. (Terence L. Chorba, et al., *Mandatory Reporting of Infectious Diseases by*

Clinicians, 262 JAMA 3018-3026 (1989) and Eugene Freund et al., *Mandatory Reporting of Occupational Diseases by Clinicians* 262 JAMA 3041-3044 (1989)).

Many public health surveillance activities are conducted without identifiable information, but some do require identifiable information. In some instances, identifiers are needed, but the information may be used only in aggregate form. This is the case with surveillance programs for certain diseases and conditions where identifiers are needed to ensure an accurate count when duplicate reports may come from different sources. But there may be no intervention, and aggregate results are produced without reference to any identified individual.

Disease registries, such as cancer registries, operate this way. State-based cancer registries are funded by the Centers for Disease Control and Prevention through the National Program of Cancer Registries (Public Health Service Act §§ 399H-399L (42 U.S.C.A. §§280e-280e4)). The Surveillance, Epidemiology and End Results (SEER) Program of the National Cancer Institute, operated since 1973, collects and publishes cancer incidence and survival data from population-based cancer registries covering approximately 14 percent of the U.S. population. It is from reports by hospitals and laboratories to these registries that we have accurate information about cancer incidence, survival rates, and geographical variations in our Nation.

Other activities important to public health and safety are conducted by bodies like the National Transportation Safety Board. It investigates airplane and train crashes, in an effort to reduce mortality and injury by making recommendations for safety improvements, and it uses medical records in its investigations. Similar inquiries are conducted by the military services.

The Occupational Safety and Health Administration, the Mine Safety and Health Administration, and the National Institute for Occupational Safety and Health also conduct public health investigations related to occupational health and safety. The Nuclear Regulatory Commission and State agencies working with it investigate occupational worker or general public radiation injury, and misadministration of radioactive materials to patients; these inquiries often require access to individually-identifiable health information. All of these activities relate to the public health and safety, and the legislation should permit disclosure for them.

Other programs, directed toward communicable disease such as sexually-transmitted disease, involve contact with the individual and provision of health care, and occasionally, enforcement actions to prevent transmission of disease. All States have authority to isolate and quarantine individuals who endanger public health. The emergence of multi-drug resistant tuberculosis has renewed attention to these powers of States. The issues are discussed in Lawrence O. Gostin, *Controlling the Resurgent Tuberculosis Epidemic*, 269 JAMA 255 (1993).

Surveillance of the effect of drugs and medical devices also involves collection of information, sometimes in identifiable form. The tracking of medical devices (under section 519 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 360i)) require that physicians report infor-

mation (sometimes including patient identifiers) to device manufacturers, and these reports may in turn find their way to the Food and Drug Administration.

The proposal envisions that disclosures will be made not only to government agencies, but also to private entities as required or permitted by law. In tracking medical devices, for instance, the initial disclosure is not to a government agency, but to a device manufacturer that collects information under explicit legal authority, or at the direction of the Food and Drug Administration. The cancer registries mentioned above are often non-profit organizations such as universities which receive reports from physicians and laboratories pursuant to State statutory requirements to report. These activities should not be impaired.

We recommend a provision for disclosure to "an individual authorized by law to receive the information in a public health intervention" so that physicians or health departments, in carrying out public health interventions authorized by law, can notify individuals who have been exposed to a communicable disease. That notification may implicitly reveal the identity of the patient, but should be permitted as a disclosure in the course of an authorized public health intervention. The recommendation does not include a confidentiality obligation on the individual notified.

The provision we recommend should sharply constrain public health agencies and other institutional entities receiving information in how they further disclose it. Public health authorities have a long ethical tradition of complete confidentiality in the conduct of their investigations, and are subject to confidentiality obligations under State law. The use and control of information by health departments is discussed in Lawrence O. Gostin, et al., *The Public Health Information Infrastructure*, 275 JAMA 1921-1927 (1996)).

The Federal legislation should bolster those ethical and legal obligations by additional safeguards. Information obtained under the public health provision should not be further disclosed except for public health purposes (which may include action against individuals, such as in quarantine situations to protect the public health, with whatever disclosure that involves), for research, or for audit or investigation of the particular public health entity holding the health information. It may also involve use and disclosure of patient information in enforcement proceedings against entities.

4. RESEARCH

We recommend that providers and payers and those receiving information under the provisions of the legislation without patient authorization be permitted to disclose health information without patient authorization for research.

We recommend that disclosures be permitted only under the following conditions:

The research would be impracticable to conduct without the individually-identifiable health information;

The research has been approved by an institutional review board organized and operated in a manner consistent with and in accord with the institutional review board requirements of Federal Policy for Protection of Human Research Subjects; and

The institutional review board has determined that disclosure is allowable without the informed consent of the subjects, and, in making that judgment, has determined that

- the research project is of sufficient importance so as to outweigh the intrusion into the privacy of the patient who is the subject of the information that would result from the disclosure;
- the research is of minimal risk;
- not obtaining consent will not adversely affect the rights and welfare of the subjects; and
- the research could not practicably be carried out if consent were required.

We recommend that a researcher receiving information be required to remove or destroy personal identifiers, at the earliest opportunity consistent with the purposes of the research, unless an institutional review board has determined that there is a health or research justification for retention of identifiers and there is an adequate plan to protect the identifiers from improper use and disclosure.

We recommend that the health information so obtained not be further disclosed except

- pursuant to a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or to the public health;
- for another research project that meets the same conditions set out in the legislation for initial research disclosure; or
- for oversight of the research project.

We recommend that information so obtained not be used or disclosed in any administrative, civil, or criminal action or investigation directed against the patient.

Health research is an integral and essential part of modern health care, and the source of much of the knowledge on which medical treatment is based. Much of that research is based on analysis of existing health records, and thus access to health records is vital to research.

Research based on health and other records has been an important source of information about the health of the population, and about how to prevent and treat disease. This research differs from research where there is an interaction with the researcher, and where the individual must of course be aware of the research and give informed consent. The latter activity may be covered as a form of health care, but is different from the records-based research for which disclosure without patient authorization is recommended here under certain conditions.

A wide variety of research activities use health records -- biomedical, epidemiological, and health services research, and statistical activities. Likewise research on behavioral, social, and economic factors affecting health, and the effect of health on other aspects of life, may use health records. Use of records in research and the privacy aspects of such research are discussed in a recent report published by the Department of Health and Human Services, *Privacy and Health Research*, a report to the U.S. Secretary of Health and Human Services by William W. Lowrance (1997). Researchers have an excellent record for maintaining confidentiality of information they get this way, and privacy has not been harmed as a result.

The Privacy Protection Study Commission, in its recommendation about health-care records, recognized the research uses of health records, and supported disclosure without patient authorization under stringent conditions, which are reflected in the present recommendations (*Personal Privacy in an Information Society* 309 (1977)).

Much important and helpful scientific knowledge has come from large-scale studies using existing records. They are discussed in Leon Gordis and Ellen Gold, *Privacy, Confidentiality, and the Use of Medical Records in Research*, 207 *Science* 153-156 (1980). Among examples of valuable research findings are these:

When mothers took DES during pregnancy to prevent a miscarriage, female offspring of these pregnancies were at increased risk of developing a rare type of cancer of the vagina when they reached adolescence.

Workers exposed to vinyl chloride are at high risk of liver cancer. This finding could only be made by reviewing the medical records of large groups of employees and linking the employees' records at the factory site with hospital records and death certificates if they existed.

The cause of increased risk of a form of blindness called retrolental fibroplasia in low birth weight infants was identified through examination of records. It was caused by high oxygen concentrations administered to premature newborns. Since this finding, use of a lower level of oxygen has virtually wiped out this form of blindness in premature infants.

The treatment of acute leukemia in children was greatly enhanced by studies of medical records that showed that new forms of therapy were effective.

Beta-blocker therapy resulted in fewer re-hospitalizations and improved survival among elderly survivors of acute myocardial infarction.

State Medicaid policies restricting the number of prescriptions per month to prevent fraud and abuse also produced large declines in use of effective medications, adverse impacts on health status, and increased utilization of more expensive health care services. With this information, several States discontinued policies that limit prescriptions per month.

The need to provide these records without contacting the patients results from the scale and type of studies using records, and their scientific characteristics. It is often impracticable, or impossible, to seek authorization from everyone in a records-based study of this kind. Some involve hundreds of thousands, and occasionally millions, of people. If it were necessary to seek authorization, some people would refuse, and some could not be found. In these cases, the people not included might have unknown common characteristics that would skew the results -- a problem that can render the results useless, and a special problem in studying rare health conditions, where a usable count depends on finding every case.

The results of these inquiries appear as statistics -- aggregate results, with analysis and conclusions -- and no one's actual identity is ever published. However, the research does depend on information about specific individuals, and in the course of the research identifiers are sometimes necessary -- to be sure that there are not duplicate reports, or to match health records with other records, like records of treatment in several health facilities or death records, to determine the long-term effects of a condition or a treatment.

In other cases, the research may call for identifying patients through existing provider records, and then contacting them and with their consent obtaining further information. There are effective techniques for contacts of this kind -- often by the provider after the researcher has identified them -- without revealing information to individuals other than the patient.

This can all be done, and is done now, without harming the patient.

Thus, we recommend that the legislation include conditions closely modeled on the regulation that protects subjects in research funded by Federal agencies, the Federal Policy for the Protection of Human Subjects (the "Common Rule," first published at 56 Fed. Reg. 28002-28032 (1991) and codified for the Department of Health and Human Services at 46 C.F.R. part 46 and

20 C.F.R. parts 50 and 56). Under this regulation, an institutional review board may waive the normal requirement for informed consent of the subjects if the research is of minimal risk, if the waiver will not adversely affect the rights and welfare of the subjects, and if the research could not be practicably carried out without the waiver (45 C.F.R. § 46.116(d)). However, we recommend that such protection be imposed by statute, and that there be criminal penalties for obtaining health information under false pretenses and for wrongful disclosure.

These conditions help ensure that records are disclosed only after careful consideration, by requiring, for example, that researchers show that patient identifiers are genuinely needed for the research and that the expected results are of sufficient importance to warrant the disclosure.

The "impracticable" test does not mean, and should not mean, that it is impossible to conduct the research in any other way, nor does it require that patient authorization be obtained if at all possible. Institutional review boards appropriately weigh such factors as cost, time and other resources available for data collection, and the quality of results.

The proposal should not oblige anyone to disclose records for research. Some providers may conclude that their records, or portions of them, are so sensitive that they should not be disclosed to outside researchers, even under the careful conditions that currently govern research and that we recommend.

It is fundamental to the protection of individuals in research that they not be disadvantaged by the research except to the extent that they know the disadvantage and voluntarily choose to accept it. The strict restrictions on further disclosure that we recommend would ensure that end. They come from this principle (called "functional separation") enunciated by the Privacy Protection Study Commission:

Information collected or maintained for a research or statistical purposes may be not be used in individually identifiable form to make any decision or take any action directly affecting the individual to whom the record pertains, except within the context of the research plan or protocol. (*Personal Privacy in an Information Society* 572-574 (1977))

5. EMERGENCY PURPOSES

We recommend that providers and payers, and those receiving information under the provisions of the legislation without patient authorization, be permitted to disclose health information without the authorization of the patient pursuant to a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual.

We recommend that disclosure be permitted only to a person reasonably likely to be able to prevent or lessen the threat.

We recommend that information so disclosed not be permitted to be used in any proceeding against the patient except for proceedings related to the reason for its disclosure, but that there be no other control on the use or disclosure of this information by the recipient, except to the extent that the recipient is otherwise covered by the law.

This recommendation addresses situations where it is necessary to disclose information to prevent harm to individuals. For example, law enforcement authorities may need information from a psychiatric record to predict the behavior of a person who is threatening others. Providers may be under an ethical or legal duty to warn someone of potential harm by a patient.

The latter circumstance has been addressed in court cases, and the provision we recommend permits disclosures in accord with cases which require disclosure, of which the leading case is *Tarasoff v. Regents of the University of California* (17 Cal. 2d 425 (1976)). In that case, a psychologist was told by a patient that the patient intended to kill a third person. The psychologist notified the police but did not warn the intended victim. The patient subsequently killed that person. The Supreme Court of California found that the therapist had an obligation to use reasonable care to protect the intended victim against danger, including warning the victim of the peril. Many States have adopted (judicially or legislatively) some type of Tarasoff duty to warn, but not all State have done so. The provision we recommend takes no substantive position on a health care provider's duty to warn, but permits the disclosure if required or allowed under applicable law.

An emergency disclosure provision does present some risks of improper disclosure, through, for example, a fraudulent telephone request with a claim that cannot be verified that information is needed for life-saving purposes. There will be pressures and uncertainties when disclosures are requested under emergency circumstances, and decisions must often be made instantaneously and without the ability to seek authorization or to perform complete verification of the request. We believe that this risk is warranted, and that the law should not hold record holders liable if they make a reasonable judgment and disclose information in good faith, even if later events reveal that the judgment was in error.

It is difficult to predict who might receive information under this provision, and so we recommend that the control on further use be formulated as a prohibition on using the information against the patient outside the occasion for the disclosure.

This provision should not otherwise control redisclosure, so that it would not, for example, burden a private individual who is notified of a threat by a patient with legal sanctions for discussing the incident. Some recipients will be health care providers, and would be obliged to comply with the legislation regardless of where the information came from.

6. STATE HEALTH DATA SYSTEMS

We recommend that providers and payers be permitted to disclose health information without patient authorization, if required or explicitly authorized by State law or regulation, for health data programs that collect health data for analysis in support of policy, planning, regulatory, and management functions identified by State statute or regulation.

We recommend that information so obtained not be further disclosed except under the same conditions and circumstances applicable to information disclosed for research purposes.

This recommendation is in support of State programs that collect data to analyze health care outcomes, quality, costs and patterns of utilization, effects of public policies, changes in the health care delivery system, and related phenomena to engage in better policy making, planning, regulation, and management. These programs frequently require reporting of information for all patients treated or released by specified classes of providers within the State. The recipient may be a State agency, or may be a private organization working in collaboration with the State. In some instances the information is reported without identifiers, but in other instances it includes some form of identifier that may make the information identifiable under the standards we propose.

The information is used to analyze trends in health care services and the costs of care. This activity partakes of the character of research, oversight, public health, and payment, but does not fall neatly into any one category. It is a valuable activity that offers the possibility of improved understanding of clinical, administrative, and financial aspects of the health care system. These benefits can be achieved while protecting the privacy interests of the patients. Like research, these activities sometimes need identifiable information, but the identity of the individuals is irrelevant to the outcome, and the results appear only in the aggregate.

For these disclosures we recommend that the data collection be required or explicitly authorized by State law or regulation. As in the case of research, the principle of functional separation formulated by the Privacy Protection Study Commission is applicable. Thus, we recommend that the restrictions on further use of this information be the same as the restrictions on further use of information disclosed for research purposes (RESEARCH, above)

7. NEXT-OF-KIN

We recommend that health care professionals involved in the direct provision of patient care be permitted to disclose health information, in connection with the patient's current treatment, to family members of the patient and others with whom the patient has a close personal relationship

- if the patient has been notified of the right to object to such disclosure and has not objected; or
- in circumstances where such notification has not been given, if the disclosure is consistent with good health professional practice and ethics.

Certain routine communications take place with a patient's family and friends in connection with illness and injury. A spouse or parent should surely be told about the condition of a patient who has been injured or suddenly taken ill. A helpful neighbor assisting an elderly person being discharged from the hospital should be informed of the person's limitations in mobility, or of a health problem that requires ongoing practical help. A roommate or friend may be dispatched to the drug store to pick up prescription medication.

In general, patients should have a choice about these disclosures, and providers should notify patients of this right, and proceed only if the patient does not object. It is not envisioned that formal written authorization will be obtained.

There may be instances where it is not feasible to notify patients, but where communication with the family is necessary. In these cases, health care professionals involved in the direct provision of patient care should have the option of using their judgment, and informing relatives as necessary, in accordance with health professional practice and ethics.

As with all permitted disclosures, providers should be able to decline to disclose in this fashion without consulting the patient. Institutions may impose on their employees policies which are more restrictive.

No further control on the use or disclosure of this information by the recipient is appropriate.

8. DIRECTORY INFORMATION

We recommend that health care providers be permitted to disclose, without patient authorization, the fact of a person's presence in a facility, and the location, and to describe the patient's conditions in general terms that do not communicate specific medical information about the patient, if the patient has not affirmatively objected in advance to these disclosures.

Hospitals and other inpatient facilities serve as temporary residences, and directory information of this type is regularly provided to verify that a person is a patient in the facility, to assist visitors to the patient, to permit mail communication, and to let persons beyond the patient's immediate circle know in a general way of the patient's condition (in terms like "good," "fair," "stable," "serious," or "critical").

Patients should be permitted to restrict such disclosures, but we do not recommend a legislative requirement for notice of this opportunity beyond the required explanation of information practices more generally (EXPLANATION OF INFORMATION PRACTICES, above). Any institution should be free to have more restrictive policies, and many might choose to ask patients explicitly whether they agree to making directory information available.

In the case of institutions which of their nature identify the condition being treated, disclosure of directory information would communicate specific medical information, and should not be permitted.

No further control on the use or disclosure of this information by the recipient is appropriate.

9. LAW ENFORCEMENT: INVESTIGATION OF PROVIDERS AND PAYERS

We recommend that providers and payers be permitted to disclose health information without patient authorization

- for investigation or prosecution of a covered entity, or
- to determine whether a crime has been committed and the nature of any crime that may have been committed, other than a crime that may have been committed by the patient,

if such disclosures are authorized by other law, and all requirement of other law have been met.

Law enforcement agencies often inquire into activities of providers and payers, and review health records in that process, without having any interest in the patients. This may occur, for example, in inquiries about compliance with tax laws, where a review of patient records might assist in estimating a provider's income, or in inquiries about compliance with safety and health laws, where review of health information might assist investigators. The patients are not the focus of the investigation and do not have an interest that warrants independent judicial consideration of the disclosure of their information. We are not recommending any changes to existing legal constraints that govern access to or use of patient information by law enforcement agencies. In addition, our recommendations would make obtaining health information under false pretenses be a Federal felony.

In other cases, health information about a victim of a crime may be needed to investigate the crime, or to allow prosecutors to determine the proper charge. For some crimes, the severity of the victim's injuries will determine what charge should be brought against a suspect. For medical information to be relevant, the crime will normally involve bodily injury to the patient. Here again, while the patient is involved, the focus of the investigation is not the patient, but someone

else. While the patient certainly has a privacy interest in the use of his or her information in the investigative process and judicial proceedings, this approach leaves control of this information to the procedures of the criminal justice system.

10. LAW ENFORCEMENT

We recommend that providers and payers and those receiving information under the provisions of the legislation without patient authorization for oversight purposes be permitted to disclose health information without patient authorization

- to investigate a crime against, or on the premises of, a health care provider or payer,
- to comply with State law that requires the reporting of specific items of health information to a law enforcement authority,
- to assist in the identification or location of a victim, witness, suspect, or fugitive in a law enforcement inquiry, in situations similar to those in which State law requires disclosure of specific items of health information to a law enforcement authority,
- upon request of a law enforcement official who states that the health information is needed for a legitimate law enforcement inquiry, and that the request complies with all applicable law, or
- upon the request of an official of the U.S. Intelligence Community, as that term is defined in section 3 of the National Security Act, 50 U.S.C. §401a, who states that the information requested is needed for a lawful purpose,

if such disclosures are authorized by other law, and all requirements of other law have been met.

We recommend that the Intelligence Community and law enforcement agencies which receive information under this provision not be subject to restrictions on its further use or disclosure, except as provided by other law.

The disclosures we recommend here are an exception to a basic principle of the protections we recommend, which is to limit the use of health information to purposes connected directly with health care and payment. It is an instance of balancing private interests and the principle of public responsibility when law enforcement agencies need access to health information. Thus, we recommend that the legislation maintain current practices by permitting disclosure of health

information to law enforcement authorities and permitting them to use that information, subject to other applicable law.

These disclosures are necessary to protect the health care system and the public, and they comport with certain well accepted realities of law enforcement and the criminal justice system. We are not recommending any changes to existing legal constraints that govern access to or use of patient information by law enforcement agencies. In addition, our recommendations would make obtaining health information under false pretenses be a Federal felony.

In instances where a crime is committed on the premises of, or against, a health care provider it may be necessary to review records. The presence of a patient in a particular location in a facility, or the timing of an observation in a chart, may help in identifying a suspect or an offense, and may incidentally disclose health information to investigators. The information needed may be limited, but could well include health information covered by the law.

State laws commonly require that health providers report gunshot wounds, injuries associated with arson, and other specific conditions. In the same vein, police typically make inquiries in emergency rooms in pursuing persons injured while committing crimes. Responses to these inquiries, even if not specifically required by law, are analogous to the reports required by law, and serve to prevent health care facilities from becoming sanctuaries for fleeing criminals. These inquiries are usually close in time to the offense and the appearance for treatment of the patient in a health care facility.

In other instances law enforcement authorities now get health information without patient consent, pursuant to other law. We are not recommending any changes to existing legal constraints that govern access to or use of patient information by law enforcement agencies. In getting information, law enforcement officials should have to comply with whatever other law was applicable. Thus, if State law permitted disclosure only after compulsory process with court review, a provider or payer should not be allowed to disclose information unless the law enforcement authorities had complied with that requirement.

We recognize that there are arguments in favor of new confidentiality restrictions to address, for example, the law enforcement possibilities in the search capabilities of computerized health records. Until more experience is gained with the nature and speed of computerization of these records, and the types and frequency of requested searches, it is premature to change existing law in this area. Existing constitutional and other legal constraints would of course remain in place.

The provision we recommend here should not permit health care providers to disclose at their own instance information about patients that is evidence of a crime (apart from crimes connected with the health care facility). The basic obligation of nondisclosure which we propose precludes this.

This provision should be permissive, and health care facilities may, as far as the protection we are recommending is concerned, choose to refuse to cooperate with requests from law enforcement authorities. However, there may be other statutes that compel cooperation of the covered entity, and the legislation should permit this cooperation.

11. JUDICIAL AND ADMINISTRATIVE PROCEEDINGS: PATIENT AS PARTY

We recommend that providers and payers and health oversight agencies be permitted to disclose health information without patient authorization

- pursuant to the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, or comparable rules of other courts or administrative agencies in proceedings in which the patient is a party and has placed his or her physical or mental condition or functional status in issue;**
- if directed by a court in connection with a court-ordered examination of an individual; or**
- to petition a court for guardianship or protective services for the patient.**

We recommend that the party seeking the information be required to give written notice in advance to the patient or patient's attorney.

We recommend that providers and payers and health oversight agencies be permitted to disclose information in these circumstances only after receiving written notification that the above conditions have been fulfilled.

The controls we recommend here of necessity intersect with existing procedural laws and rules of Federal and State courts and administrative agencies. We recommend that the legislation impose procedural controls on disclosure of information in these circumstances, but leave substantive judgments about use of the health information to the law governing the proceeding. In this type of proceeding, the patient's privacy interest is necessarily more limited than one in which the patient is not already a party, and in addition the patient is in a position to seek appropriate restrictions from the court. This provision for disclosure is intended to apply to administrative proceedings, such as appeal processes in Federal benefit programs.

Our recommended procedure is meant to provide assurance to providers and payers that disclosure is proper, and to give notice to the patient. A person seeking health information should be required to notify the patient or the patient's attorney of the request, and to give the holding entity

a signed document attesting to this notification, and to give sufficient time to permit the patient to challenge the request.

In particular, such a provision would provide an opportunity to object to demands for information where the patient may have a proper claim that the request for information is too sweeping, or that the information is irrelevant to the proceeding. Some litigation reasonably requires medical information, but the patient's entire past medical history may not be relevant to the issue at hand, and its disclosure may be an inappropriate invasion of privacy. This procedure would ensure notice to the patient, and an opportunity to object in a timely fashion under the rules applicable to the proceeding.

The dispute about the need for the medical information or the scope of the request could then be resolved by the tribunal considering the matter. The general rule that disclosures must be limited to the minimum amount of information necessary to accomplish the purpose for which the information is to be used should be fully applicable, and this rule could thus be used by patients to contest the scope of discovery requests.

12. JUDICIAL PROCEEDINGS: OTHER

We recommend that providers and payers be permitted to disclose health information in a judicial or administrative proceeding (other than a proceeding in which the patient is a party and has put his or her condition at issue), pursuant to an administrative or judicial subpoena if the patient has been notified in advance and has not objected in a timely manner.

We recommend that if the patient has been notified in advance and does object in a timely manner, the official issuing the subpoena not order the information disclosed unless the person seeking the information has demonstrated that

- there are reasonable grounds to believe that the information will be relevant to the proceeding; and
- the need for the information outweighs the privacy interest of the patient.

We recommend that in determining whether the need for the information outweighs the privacy interest of the patient, the court or agency consider

- the particular purpose for which the information was collected;
- the degree to which disclosure of the information will embarrass, injure, or invade the privacy of the patient;

- the effect of the disclosure on the patient's health care;
- the importance of the information to the lawsuit or proceeding; and
- any other factor deemed relevant by the court.

We recommend that a covered entity be permitted to challenge a demand for health information on any grounds available under this or other law.

This recommendation addresses the need for health information in proceedings other than proceedings in which the patient is a party.

The procedure we recommend is basically the same as for those situations. The test for disclosure is somewhat different, in light of the need to demand a higher degree of justification for seeking health information in proceedings that are not law enforcement proceedings, or in which the patient is not already before the court.

13. JUDICIAL PROCEEDINGS: INFORMATION OTHERWISE ALLOWED TO BE DISCLOSED

We recommend that disclosure be permitted without notice to the patient, or judicial determination, if the health information could be disclosed under other provisions of the legislation not requiring notice or judicial determination, provided that the conditions in the other provisions are satisfied.

The procedural safeguards attendant to disclosure of health information in judicial proceedings should not be required when the information could be disclosed under other provisions without judicial proceedings.

In these instances, the requirements of the other sections authorizing the disclosure provide safeguards for the individuals. Notice to individuals simply because compulsory process was being used would serve no useful purpose and might wrongly convey the impression that the patient was somehow being investigated.

Disclosures that we propose be permitted without patient authorization are sometimes in fact made pursuant to compulsory legal process required or authorized by other law. Health oversight agencies have this authority (discussed in the **HEALTH OVERSIGHT** section, above). State and local public health agencies have subpoena or warrant authority to obtain information. The Occupational Safety and Health Administration and the National Institute for Occupational Safety and Health have authority to compel disclosure of health records for their public health and safety investigations and occupational health and safety research (29 U.S.C. §§657, 669), and the Mine Safety and Health Administration (30 U.S.C. §813) has similar

authority. Should agencies with that authority have to use it, they should not be required to comply with the notice and judicial determination requirements applicable in other proceedings using compulsory process.

The legislation should also provide that, if disclosure is conditioned upon a requirement to disclose in State law, Federal agencies may make the disclosure despite the inapplicability of State law to their activities.

F. SPECIALIZED CLASSES OF PERSONS AND ENTITIES

1. DECEASED PERSONS

We recommend that patients be covered by the protections of the legislation for two years after death, and that the right to control the patient's health information within that time be held by an executor or administrator, or in the absence of such an officer, by next-of-kin, determined under State law, or in absence of both, by the holder of the health information.

Whether to apply confidentiality legislation to information about deceased patients is a difficult issue, with good arguments in favor both of protecting and not protecting this information. In traditional privacy law, privacy interests, in the sense of the right to control disclosure of information about oneself, cease at death. The underlying purpose of health record confidentiality -- to encourage a person seeking treatment to be frank in the interest of obtaining care -- may require, from the patient's perspective, confidential treatment of information even after death. However, the problem of ensuring confidentiality after death is complicated by the traditional method of managing affairs after death -- control by an executor or administrator, who is often a relative. The result may be that the very people the deceased may have hoped would not know of his or her health condition will control the information.

At the same time, perpetual confidentiality has serious drawbacks. If information is needed for legitimate purposes, there should be someone legally authorized to disclose it, by analogy with authorization by a living person. A permanent bar to disclosure would serve privacy interests only rarely, and could interfere with important and acceptable uses of information, such as historical research.

A two year period of confidential treatment, with provisions for authorization by specific persons, would preserve dignity and respect by preventing uncontrolled disclosure of information immediately after death but permitting disclosure for proper purposes during this period. It should be noted that providers may, apart from legally compelled disclosure, choose to keep information confidential for a longer period.

2. IDENTIFICATION OF DECEASED PERSONS

- We recommend that health information be permitted to be disclosed to identify a dead person, or to aid a medical examiner's or coroner's investigation.**

Information from health records is used to identify dead persons, and this recommendation permits providers and payers to disclose information for this purpose. In an instance where information so disclosed reveals information about a living person, that information should not be used for any purpose relating to the living individual.

Medical records are used in investigation of causes of death, and should be permitted to be disclosed for that purpose.

3. CORRECTIONAL AND DETENTION FACILITIES

We recommend that health information about patients who are inmates of correctional facilities, or incarcerated in detention facilities, be available to prison and detention officials responsible for the custody and care of the inmates and detainees, and that no further restrictions apply to the use and disclosure of this information. We recommend that the rights and obligations of the legislation not apply to inmates or detainees, or the officials or entities responsible for their care and custody.

This recommendation acknowledges the special situation of persons in correctional facilities, whose health care is a fundamental responsibility of the officials of those facilities.

4. MINORS

We recommend that patients below the age of 18 who, acting alone, have the legal capacity to apply for and obtain health care and who have sought such care, should have all rights under the legislation with respect to information relating to such care.

We recommend that in cases not covered by the preceding condition, and in which the patients is age 14, 15, 16, or 17, either the patient or the parents or legal guardians be authorized to exercise all rights under the law.

We recommend that the rights of patients under 14 years of age be exercised by the parent or legal guardian of the patient.

These recommendations recognize the special situation of minors. They take into account the responsibility and concern of parents for their children, and at the same time acknowledge the

ability under many State laws of minors to consent to their own care for particular conditions named in statute.

5. POWERS OF ATTORNEY

We recommend that persons authorized by law (other than on account of minority) to act for a patient, or authorized by an instrument recognized under law, to act as agent, attorney, proxy or other legal representative, exercise all rights of the patient to the extent authorized by the grant of authority.

We recommend that persons authorized by law, or by an instrument recognized under law, to make decisions about a patient's health care exercise the rights of the patient to the extent necessary to effectuate the terms or purposes of the grant of authority.

These recommendations address situations in which patients have formally authorized others to act for them, or are unable to act for themselves. They are necessary accommodations in situations where, for purposes beyond decisions about information, others are acting for patients.

As it relates to persons authorized to make health care decisions for others, this recommendation recognizes the power, under the laws of most States, of individuals to designate others to make health care decisions on their behalf, in the form of durable powers of attorney or similar instruments. The definition of rights we recommend is similar to one offered by the National Conference of Commissioners on Uniform State Law, in the Uniform Health-Care Decisions Act (9 Part I U.L.A. 93 (Supp. 1994)) in this circumstance.

6. PATIENTS UNABLE TO MAKE CHOICES FOR THEMSELVES

We recommend that if a patient is not capable of exercising his or her rights under the legislation but has not been legally adjudicated as incompetent or has not had a legal representative appointed, the patient's rights under the recommended Federal privacy act be exercised by a person who holds a health care power of attorney for the patient, or in the absence of such a person, by next of kin, or in the absence of such a person, the health care provider.

We recommend that anyone exercising these rights be required to do so in the best interest of the patient.

This is intended to deal with situations where a patient is unable to exercise the rights under the confidentiality law, and there is no formal legal arrangement for others to exercise those rights.

7. BANKING AND PAYMENT PROCESSES

- We recommend that providers and payers be permitted to disclose, in connection with payment by debit, credit, or other payment card or account number, or other electronic payment means, the minimum amount of health information necessary to complete the payment transaction.

We recommend that a debit, credit, or other payment card issuer, or anyone otherwise directly involved in payment or billing transactions through such means, be permitted to use or disclose health information about a patient only for authorization, settlement, billing or collection, and for other purposes directly related to these financial operations.

Financial organizations such as banks that issue credit cards now process payment for health care. In the course of making payment for health care, and billing customers, they may incidentally receive health information. When a patient pays a provider using a credit card, the transaction does not use health information as such, and the provider should not include health information in communicating with the bank to receive payment.

However, some health information can be derived by ready inference from information that is included in the financial transaction. The specialty of a provider, which is easily determined, may indicate the type of health care being received. The amount or pattern of charges may suggest with some precision the gravity or character of a patient's condition.

Any health information so disclosed should be used only for the immediate purposes of the transaction.

Since entities performing these functions are typically regulated as financial or credit institutions, and transactions with health information are integrated into their more general operations, there is no value in identifying them as payers or service organizations and subjecting them to the range of obligations imposed on providers and payers and their service organizations.

The legislation should prevent them from using identifiable patient information for purposes beyond the immediate transactions. In particular, they should not be allowed to use health information for purposes like direct marketing by the processor or by others, for the development of consumer profiles, for prescreening, for credit evaluation, or for other purposes.

The limitations we recommend should not interfere with use of patient information in audits, transfer of receivables or accounts, or the range of activities that surround the sale or transfer of receipts, or any legal or regulatory access to information that is common to the transactions of the processor more generally. The intent is to prevent the use of health information as such for any purpose beyond those narrowly connected with payment.

8. DISCLOSURES WITHIN THE DEPARTMENT OF VETERANS AFFAIRS

- We recommend that disclosures of health information within the Department of Veterans Affairs for the purposes of the benefit programs of that Department be permitted without explicit authorization.**

In the Department of Veterans Affairs health information about its beneficiaries currently flows as necessary from its medical facilities to its benefits payment elements, to permit benefit determinations based on health status. There is little value in requiring, for these information transfers within that agency, that veterans give the same authorization they would have to provide, for example, to permit disclosure of a private provider's records to a private insurance company. Simplicity and convenience for the veterans, and reduction of merely formalistic documentation, warrant this exception to the authorization requirements. The Privacy Act of 1974 provides a structured framework for the maintenance of the information, and existing confidentiality statutes cover DVA information without distinguishing health information from other information (38 U.S.C. § 5701).

9. MILITARY SERVICES — MEMBERS

We recommend that the Secretaries of Departments including military services be authorized to promulgate regulations permitting disclosure without patient authorization of health information about members of the military services, by health care providers and payers that are part of the military services or operating on behalf of the military services.

The purpose of the health care system of the military services differs in its basic character from that of the health care system of society generally, and the leadership of the military services has a special relationship with its members. The special situation of the military services is acknowledged by the Constitutional provision for separate lawmaking for them (U.S. Const. art. I, § 8, cl. 14), and in their separate criminal justice system, under the Uniform Code of Military Justice (10 U.S.C. §§ 801 et seq.)

Officials of the military services are responsible for the health of the members, and use information, including health information, to make operational choices about assignment of personnel and other matters relating to the national defense functions. Examples include the medical status of pilots, the reliability of nuclear weapons personnel, and compliance with controlled substance policies. The normal role of the patient in authorizing disclosure of health information would be inconsistent with these responsibilities and relationships, and thus we recommend that the military departments be permitted to modify the disclosure rules as necessary.

Under this recommendation, the rules could be modified for providers and payers which are direct military activities, as well as for civilian facilities serving members of the military services pursuant to contract (such as TRICARE managed care support contractors). We recommend that

the authority to modify the disclosure rules apply only to health information about members of the military services.

The legislation should not permit promulgation of regulations to permit disclosure or use of information that is restricted or controlled by other law.

This recommendation is applicable to the Department of Defense and the Department of Transportation.

10. MILITARY SERVICES – CIVILIAN EMPLOYEES AND CONTRACTORS

We recommend that the Secretaries of Departments including military services be authorized to promulgate regulations restricting the revocation of authorizations for disclosure of information by civilian employees and contractors' employees in instances where ongoing access to health information is necessary for the conduct of national defense functions.

This provision addresses the situation of civilian employees of the military services, and contractor personnel, who authorize use of their health records to evaluate their suitability for deployment and other defense-related activities. Information about their health is needed on a continuous basis, and revocation of the authorization would interfere with use of the information, possibly in situations where the lack of information could have serious operational consequences.

G. RELATIONSHIP TO OTHER LAW

1. CERTAIN LAWS NOT AFFECTED

We recommend that the legislation not preempt, supersede, or modify the operation of

- any law that provides for the reporting of vital events such as birth and death;**
- any law requiring the reporting of abuse or neglect of any individual;**
- the provisions of the Public Health Service Act regarding notification of emergency response employees of possible exposure to infectious diseases (Public Health Service Act subpart II, part E, title XXVI (42 U.S.C. §§ 2681-2690);**
- any law requiring or explicitly authorizing the reporting of injuries or illnesses in connection with a workers' compensation program; or**

— any law that establishes a privilege for records used in health professional peer review activities.

These activities are all subject to existing law, and we recommend that they not be affected at all by the legislation. This proposal is not simply that disclosures to comply with these laws be allowed: it is that these disclosures and activities under these should not be affected at all.

The reporting of vital events like birth and death may include health information, but the reports are made pursuant to an existing body of law which controls use of the information so disclosed, and are for public purposes beyond health care. All States have laws in this area, many based in whole or in part on the model statute promulgated by the National Center for Health Statistics (Centers for Disease Control and Prevention, National Center for Health Statistics, *Model State Vital Statistics Act and Regulations* (1992)).

The reporting of neglect or abuse is addressed by law in every State.

In workers' compensation programs, State laws require employers to report injuries to State agencies or workers' compensation insurance carriers. While in many cases these reports will come from employers and will not include health information, there will be instances in which a health care provider will make the report. The legislation should not affect these reports.

To the extent that health information is used in health professional peer review activities, control of its use and disclosure should be left to the specialized statutes governing those activities.

2. PRIVILEGE STATUTES

We recommend that a patient's authorization for disclosure of health information for health care or payment, or disclosure under the legislation for those purposes without patient authorization not diminish, waive, or otherwise impair any testimonial privilege.

Existing privileges, which in some instances can be abrogated by disclosure of the information covered by the privilege, should be preserved.

3. THE PRIVACY ACT OF 1974

We recommend that providers and payers now subject to the Privacy Act of 1974 remain subject to that Act.

We recommend that these providers and payers be obliged to observe the disclosure restrictions of federal privacy legislation as well as any disclosure restrictions of the Privacy Act that are more restrictive than such legislation.

We recommend that Federal agencies be permitted to make disclosures now allowed by the Privacy Act to the National Archives and Records Administration.

The Privacy Act of 1974 (5 U.S.C. § 552a) was a pioneering statute for the use and control of personal information, and continues to serve the public well as a control on the use and disclosure of information by the Federal government. Its significant contribution to privacy interests are its requirements that agencies maintain only information necessary to the agencies' purposes; that individuals have the right to access and to request amendment of their records; and that agencies be open about the records they keep and their uses and disclosures.

Written to cover the wide variety of records found in the entire Federal government in 1974, including many of minimal sensitivity, its use and disclosure provisions are not highly restrictive. The Act explicitly identifies many disclosures as allowable without individual consent. Information may be used by employees of an agency who have a need to know the information to perform their duties, and "agency" includes an entire cabinet Department. Information may be disclosed pursuant to court order and pursuant to proper requests from law enforcement authorities, and to certain other Federal agencies. There are several other specified allowable disclosures. Beyond those set out in the text of the Act, agencies have discretion to make other disclosures through their administrative power under the Act to establish, by notice, comment, review by the Office of Management and Budget and Congress, a routine use -- a disclosure of information outside the agency "for a purpose which is compatible with the purpose for which it was collected." In devising their routine uses agencies have latitude in determining what is "compatible," although the courts have been looking more closely in recent years at agency choices.

Many Federal agencies conduct activities that would be covered by the legislation we recommend, such as the provision of care by the Clinical Center of the National Institutes of Health, the hospitals and clinics of the Department of Veterans Affairs, the Department of Defense and the Indian Health Service, and the payment activities of Medicare and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS).

We recommend that federal health record confidentiality legislation limit the latitude of these agencies to make the disclosures otherwise permitted by the Privacy Act. Federal agencies should be restricted in their intra-agency disclosures, and in promulgation of routine uses, to the purposes and uses set out in the health privacy legislation we recommend.

This recommendation is based on these principles:

Health information is a specialized class of information that deserves the more careful treatment, in terms of disclosure restrictions, that the legislation we now recommend would provide.

Federal and other (private, State and local government) health care and payment activities ought, as much as possible, to be subject to the same confidentiality rules.

A common set of rules for health records in all health programs is more important than a common set of rules for records whose only similar feature is their Federal maintenance.

At present, existing confidentiality statutes are often overlaid on the Privacy Act, with the effect that the protections are cumulative. That is the result sought here, and it should be addressed explicitly in the law.

There are strong reasons to encompass both Federal and other health records within a common protective scheme. There is increasing interaction among the Federal, private, and State government sectors in sharing of facilities, purchase of care, and the like. The work of all these facilities and their personnel would be simplified by a common set of rules.

We recommend that the proposal leave in place the subject access and amendment provisions of the Privacy Act, and that it not diminish any protections against disclosure provided by that Act. Unforeseen circumstances can be accommodated under the administrative authority we recommend, below (discussed under **AUTHORITY FOR LIMITED SUSPENSION**).

The archives provision deals with the special situation of Federal agencies whose records are subject to the Federal Records Act.

4. STATE LAW

We recommend that the legislation preempt State laws only to the extent that those laws are less stringent or restrictive than the Federal law.

We recommend that the Federal legislation supersede State law only when the State law is less protective than the Federal law. If either the Federal or State law forbids a disclosure, the disclosure should not be permitted. Thus, the confidentiality protections would be cumulative, and the Federal legislation would provide "floor preemption."

Generally, Federal statutes that provide rights to individuals with respect to privacy and liberty do not displace stronger State laws, and we believe that the legislation we recommend should follow that tradition.

We are aware of the strong arguments, and repeated recommendations, that Federal law in this area should be totally preemptive, i.e., that it totally occupy the field of protection of health care information, so that no State could maintain or establish any law governing use and disclosure of health information.

Those arguments are based on the increasing integration of the health care information system in this country, in which information passes easily from State to State, when information generated in one State may with ease be retrieved in another State, and when it is difficult even to identify the "location" of information to determine which State's law applies.

Nevertheless, we have concluded that the careful attention States have given, and continue to give, to this issue, should be respected. Some States have comprehensive health confidentiality statutes analogous to the one recommended here, and others are considering them. Many have carefully designed statutes protecting specialized classes of information, particularly information about AIDS and HIV infection patients, and mental health patients.

The Federal protection would ensure that everyone has an adequate level of privacy protection, and if the people of the several States wish more, or see special privacy needs which are not being met, they can retain or enact additional safeguards.

5. OTHER LAW GOVERNING HEALTH INFORMATION

We recommend that the legislation not modify or supersede other Federal or State law that provides greater protection.

Some health information subject to the legislation we recommend will also be subject to other law restricting its use and disclosure. The subjects of this information ought to have the benefit of all applicable law.

This may be the case with information held by payers and providers, in States with more protective statutes for some elements of health information (as discussed above in STATE LAW), and will be the case with some information held by Federal agencies. It may also be the case with information disclosed by payers and providers under provisions of the legislation without patient authorization.

In the latter instance, the information would, in its new setting, become subject to other statutes as well as the redisclosure provisions of the legislation we recommend. For example, information disclosed for research may become subject to statutes governing certain statistical activities (Public Health Service Act § 308(d), 42 U.S.C. § 242m(d)), health services research activities of the Agency for Health Care Policy and Research and its grantees and contractors (Public Health Service Act § 903(c), 42 U.S.C. § 299a-1(c)), or research subject identity protection (Public Health Service Act § 301(d), 42 U.S.C. § 241(d)). In other instances, State law may also restrict the disclosure of this information.

In the case of Peer Review Organizations, which review health information to ensure the quality of care for Medicare beneficiaries, health information is protected by its authorizing statute (Social Security Act § 1160, 42 U.S.C. § 1320c-9).

The Americans with Disabilities Act prohibits discrimination on the basis of disability, and in regulating the assessment of applicants and employees, requires employers, among other things, to keep medical information "on separate forms and in separate medical files" and to treat this "as a confidential medical record." (§§ 102(c)(3) and (4), 42 U.S.C. §§ 12112(c)(3) and (4)). Section 503 of the Rehabilitation Act of 1973, 29 U.S.C. § 793, provides the same protections for Federal contractor employees and job applicants (regulation at 41 C.F.R. § 60-741.23).

These laws should continue to apply. Information obtained by employers in providing health care or payment should be subject to the legislation we propose. Information subject to the Americans with Disabilities Act or Rehabilitation Act (whether or not obtained in treatment or payment) should continue to be covered by these laws. There should be no conflict between the requirements, since neither those laws nor the legislation we recommend requires any disclosure that violates the other law.

In providing for the continuance of stronger State law, the legislation should not modify the scope of the Employment Retirement Income Security Act of 1974 (ERISA) (29 U.S.C. § 1134) preemption of State laws. We recommend new minimum federal standards that would apply to many different entities that hold health information, including ERISA plans. However, we are not recommending that States be given new authority to apply more protective privacy standards to ERISA plans.

6. FEDERAL SUBSTANCE ABUSE CONFIDENTIALITY STATUTE

We recommend that the Secretary of Health and Human Services be authorized to determine, by regulation, which elements of the Federal substance abuse confidentiality statute ((Public Health Service Act § 543, 42 U.S.C. § 290dd-2) should continue to apply, so that the net effect of that statute and the one recommended will be at least as strong protection for the information concerned.

We recommend that the Secretary of Veterans Affairs be similarly empowered with respect to the statute governing substance abuse, sickle cell disease, and HIV infection in the records of the Department of Veterans Affairs (38 U.S.C. § 7332).

This recommendation will ensure that the strongest protections of the new legislation and the existing laws will both apply to covered information. The relevant Cabinet Secretaries would publish regulations to specify what rules apply.

H.

ENFORCEMENT

1. CIVIL

We recommend that any patient whose rights have been violated knowingly or negligently be permitted to bring an action, in a U.S. District Court or any court of competent jurisdiction for actual damages and for equitable relief. We recommend that actual damages encompass nonpecuniary losses such as physical and mental injury as well as pecuniary losses. We recommend that in the case of knowing violation, attorneys' fees and punitive damages should be available.

We recommend that common law liability be eliminated for any disclosure that is permitted by the legislation we recommend and is not otherwise prohibited by State or Federal statute.

We recommend that members of institutional review boards and their parent entities not be liable for a good faith determination of the propriety of a disclosure for research under the provisions allowing for such disclosure.

We recommend that there be no liability for a disclosure based on good faith reliance on a certification by a government authority or other person that a requested disclosure is in accord with the law.

The ability to seek redress for violations is an important element of confidentiality protection. There have been, and will continue to be, improper disclosures of health information, through negligence or deliberate choice. The victims of such disclosures should be able to seek civil redress.

The Privacy Working Group of the President's Information Infrastructure Task Force identified this as a basic principle in its *Principles for Providing and Using Personal Information*:

III.C. Redress Principle

Individuals should, as appropriate, have a means of redress if harmed by an improper disclosure or use of personal information.

The President's statement on the Global Information Infrastructure, *A Framework for Global Electronic Commerce* (June 1997) reiterates this point:

Under these principles, consumers are entitled to redress if they are harmed by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information.

Other statutes establishing confidentiality obligations provide a cause of action, such as the Fair Credit Reporting Act, which permits suits in the U.S. District Courts, or in any other court of competent jurisdiction, to enforce liabilities under that act (15 U.S.C. §§ 617-618). Cable television operators are forbidden to disclose subscriber information except under defined circumstances, and violations give rise to civil liability, with a cause of action in the U.S. District Court (47 U.S.C. § 551(f)). The wrongful disclosure of video tape rentals or sales information gives rise to a similar cause of action (18 U.S.C. § 2710(c)). New restrictions on disclosure of State motor vehicle information were imposed by the Violent Crime Control and Law Enforcement Act of 1994, and individuals have a cause of action in the U.S. District Court against persons who obtain or disclose information in violation of the restrictions (Pub. L. No. 103-322, § 300002, 108 Stat. 1796, 2101, 18 U.S.C. § 2724).

We recommend that the legislation take a balanced approach that compensates, in the case of negligence, only for actual losses, although not only monetary losses. In the case of a knowing violation, punitive damages and attorneys' fees should also be available.

Our recommended definition of actual damages envisages better recovery possibilities than the Privacy Act of 1974, whose damages provisions (subsections (g)(1)(D) and (g)(4))) have in some instances been read to mean only pecuniary damages, and whose standard for recovery is that the Federal agency acted intentionally or wilfully ((g)(4)). The Privacy Protection Study Commission, responding to a specific Congressional request to address this issue, recommended expansion of the Privacy Act recovery to both special and general damages (*Personal Privacy in an Information Society* 530-1 (1997)). The limitations of the Privacy Act in providing satisfactory remedies has been noted by various commentators, including Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law* § 5-5(a)(1996).

We recommend that the rights provided by the legislation be enforceable in any court of competent jurisdiction, as in the case of the Fair Credit Reporting Act, and we recommend that there be nothing to prevent States from providing other remedies in State law for violation of the Federal law.

We recommend that recovery for the wrongful behavior of public employees acting in an official capacity be against their agencies, in accord with current law.

Some current enforcement of privacy rights occurs through litigation under common law theories of a general public policy of medical confidentiality (derived from privilege and licensing statutes), contract, malpractice, and tortious invasion of privacy. Federal confidentiality legislation should bring certain and uniform standards to the redress and recovery process, and thus we recommend that there be no common law recovery for uses and disclosures of information permitted by the Federal law and not otherwise prohibited.

These recommendations are intended to protect record holders and those who assist in making determinations about disclosures against liability based on those disclosures if they act in good

faith. Record holders should be able to, but should not have to, make their own inquiries into requests for allowable disclosures in the absence of a social irregularity in the request.

2. CIVIL MONEY PENALTIES

We recommend that there be authority to impose civil money penalties on any covered entity which has demonstrated a pattern or practice of failure to comply with the provisions of the law.

We recommend this additional remedy for grave or continuing offenses. The procedural aspects of the penalties could be similar to those for wrongdoing in the Medicaid and Medicare programs, under section 1128A of the Social Security Act.

3. ALTERNATIVE DISPUTE RESOLUTION

We recommend that the alternative dispute resolution procedures be available for disputes giving rise to civil liability under the law.

4. CRIMINAL PENALTIES

We recommend criminal penalties (including fine and imprisonment) at the felony level for obtaining health information under false pretenses, for knowing and unlawful obtaining of health information, and for knowing and unlawful use or disclosure of health information.

We recommend that the penalties be higher for any of these acts performed for profit or monetary gain.

Activities that should violate the law would be requesting or obtaining health information under false pretenses from a covered entity; knowingly obtaining protected health information with the intent to sell, transfer, or use the information for profit or monetary gain; knowingly selling, transferring, or using health information for profit or monetary gain; or knowingly using or disclosing health information in violation of the law's requirements for nondisclosure.

The penalties we recommend are modeled on the penalties provided in the Health Insurance Portability and Accountability Act of 1996 for violation of disclosure restrictions in the administrative simplification provisions of that Act (Social Security Act § 1177, 42 U.S.C. § 1320d-6).

I. ADMINISTRATION

1. IMPLEMENTATION

We recommend that the legislation provide authority to issue regulations to implement the legislation.

We recommend that there be authority to

- sponsor research relating to the privacy and security of health information;
- develop information and technical guidance for protection of health information; and
- develop technology to implement standards regarding health information.

We recommend that there be authority to promulgate

- model notices of information practices for use by entities subject to the legislation;
- model authorizations for disclosure and model statements of intended use of health information by persons requesting that patients authorize disclosure of health information;
- guidelines for the administrative, technical, and physical safeguards required to protect health information;
- guidelines for what levels and amounts of information constitute "identifiable" information, and guidelines for minimum allowable disclosures in particular situations;
- guidelines for use within organizations of health information "only for purposes compatible with and directly related to the purposes for which the information was collected or received";
- requirements for institutional review boards authorized to approve disclosures for research;
- model notices to advise patients of efforts to obtain health information in legal proceedings; and

- **standards for electronic and magnetic writings that would fulfill the requirements of the legislation.**

This recommendation recognizes the need for interpretation and application when new confidentiality standards govern health information. An ongoing Federal authority is needed to preclude doubt and confusion, to provide certainty in applying the rules, and to be a point of public reference and recourse with respect to violations subject to civil money penalties.

In addition, there should be authoritative sources for technical guidance for several matters that cannot be addressed in detail in legislation. Entities subject to the legislation should be assured that they are in compliance if they used model notices, security practices, and other forms and techniques promulgated centrally. In some areas, like restricting use of health information to the purposes for which it was collected, new organizational and administrative techniques could be promulgated to assist small businesses to comply.

2. AUTHORITY FOR LIMITED SUSPENSION

We recommend that there be authority to suspend, by regulation, any provision of the legislation for a limited period in the event of an unforeseen significant threat to health or safety, significant threat to patient privacy, major economic disruption, or manifest unfairness.

The design of precise controls on the use and disclosure of information is a complex task, and it is possible that the legislation would forbid a disclosure, or otherwise constrain behavior, in a way that causes unanticipated hardship.

Authority to suspend a provision would ensure that situations like this could be addressed, on a temporary basis, pending Congressional consideration of amendments.

Federal agencies are accustomed to the flexibility provided by the Privacy Act of 1974, whose routine use provision (5 U.S.C. § 552a(a)(7) and (b)(3)) permits agencies to make administrative choices to disclose information beyond the disclosures explicitly allowed in the statute. We do not recommend administrative authority as flexible as the routine use provision, which appears in a law covering all activities of all Federal agencies, and where a statutory catalog of all possible uses of information was not feasible. We recommend a provision to deal with extraordinary situations that may have not been foreseen, and then only for a limited time.

3. EFFECTIVE DATE

We recommend that the obligations of the providers and payers become effective 9 months after the promulgation of implementing regulations.

We recommend that there be authority to exempt records in existence on the date of enactment from compliance with specific provisions of the law, for time-limited periods.

These recommendations are for an implementation schedule to ensure adequate time to apply the rules to health information in the hands of providers and payers.

The requirements we recommend can be applied with minimal trouble to new transactions with patients and to records developed with the legislation as background and guidance. At the same time, to apply the legislation to existing records, including some that are in archival status, could present undue hardships, with little benefit to patients. It is not intended that patients whose records exist already should not get the protection of the law. The exemption provision should be available only for situations where there is no significant adverse privacy effect on the patient.

III.

CONCLUSION

Thomas Jefferson said: "Our laws and institutions must keep pace with the progress of the human mind." We believe that these recommendations should be the first -- not the last -- chapter in an on-going bipartisan process to safeguard our citizens' right to health care privacy in an ever-changing world.

Ultimately, we must judge ourselves by whether we leave the next generation with real federal privacy standards grounded in fundamental principles. Will we have boundaries to ensure that, with very few exceptions, our health care information is used only for health care? Will we have assurances that our information is secure? Will we have knowledge about and control over what happens to our health care records? Will those who violate our privacy be held accountable -- and those who are violated be able to seek redress? Will we be able to safeguard our privacy rights while still protecting our core public responsibilities like research, public health, and law enforcement?

In short, will we be able to harness these revolutions in biology, communications, and health care delivery to breath new life into the trust between our patients and their doctors, between our citizens and their government, between our past and our future. We can. And, if we work together and act quickly, we will.

**Side by Side Comparison of
the February Discussion Draft of the “Medical Information Confidentiality Act of 1998” (Bennett/Jeffords) and
S. 1368, the “Medical Information Privacy and Security Act” (Leahy/Kennedy)**

TOPIC	Bennett/Jeffords	Leahy/Kennedy
PURPOSE	To establish federal <i>confidentiality</i> protections for personally identifiable health information. (p. 4)	To establish a <i>right to privacy</i> in personally identifiable health information. (p. 9)
COVERED ENTITIES	Each section of this Act specifically lists the entities that it covers. The entities covered vary from section to section, but generally include: <i>health care providers, health plans, health oversight agencies, public health authorities, employers, health or life insurers, schools, and universities, health researchers, and law enforcement agencies.</i> (throughout the bill)	Same, except that <i>health researchers</i> are included in more sections in this Act. (throughout the bill)
PROTECTED HEALTH INFORMATION (PHI): DEFINITION	Protected health information (PHI) is any information collected from an individual in any form that is created or received by a health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, school, or university <i>that relates to the individual's health condition (including individual cells and their components), care or payment, and could identify the individual</i> or a reasonable basis exists to believe that it could be used to identify the individual. ¹ Information collected by <i>health researchers</i> is not included. (p. 16)	Essentially same definition, but explicitly states that <i>genetic information</i> is included (as well as individual cell and cell components). In addition, <i>health information created or received by health researchers</i> is covered. (pp. 15-16)

¹As drafted, the bill includes *only* PHI that has been provided in an encrypted format. (See p. 17, l. 22--use of the word “and.”)
This word choice is presumably a typographical error.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
HEALTH CARE OPERATIONS: DEFINITION	Health care operations are defined as: services provided by or on behalf of a health plan or provider <i>to carry out management functions or to implement the terms of a contract for benefits</i> , including coordination of care, conducting quality assurance, reviewing competence or qualifications of providers, performing accreditation, licensing or credentialing; analysis of claims or records; evaluating plan performance; carrying out utilization review, precertification, or preauthorization of services; underwriting or experience rating of health plans; conducting or arranging for auditing services; or <i>comprehensive health care management of the individual including risk assessment, prevention intervention, case management, disease system management, continuous quality research and improvement initiatives, development of best case clinical guidelines and all other health care services necessary to ensure the optimal care of the individual.</i> (p. 7)	The term “health care operations” is not included in this bill.
HEALTH OVERSIGHT AGENCY: DEFINITION	A <i>health oversight agency</i> is (1) a person who performs or oversees an evaluation relating to licensing, accreditation, or credentialing of health care providers; or (2) a person who performs an audit or evaluation relating to compliance with legal, fiscal, medical, or scientific standards of performance related to the delivery of or payment for health care; [or] ² a public agency, a person acting pursuant to a requirement of such an agency, or a person carrying out Federal or State required activities regarding licensing, accreditation, or credentialing. (p. 9)	A person who performs an assessment, evaluation, or prosecution relating to compliance with legal or fiscal standards dealing with health care fraud and is a public executive branch agency, acting pursuant to a requirement of such an agency or its agent, or carrying out activities under Federal or State law regarding the assessment, evaluation, determination, investigation, or prosecution relating to the compliance with standards dealing with health care fraud. (pp. 13-14)

² The draft strikes the word “and,” but it is difficult to understand the definition without such a term.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
HEALTH RESEARCHER: DEFINITION	A person, officer, employee, or independent contractor of a person who receives PHI as part of a Federally qualified research project or receives PHI as part of a research project that is subject to the confidentiality provisions of this Act. (p. 11)	A person who receives PHI pursuant to health research (as described in this Act) or while acting in the capacity as an officer, employee, or agent of a person who receives such information pursuant to health research. (p. 14)
AGENT: DEFINITION	A person who represents or acts for another as an agent or under a contract or whose function is to affect contractual obligations between the principal and a third party, including a contractor. (p. 5)	Essentially same definition, exception focuses on employees of a person whose function is to affect contractual obligations and not a contractor. (p. 11)
INSPECTION AND COPYING OF PROTECTED HEALTH INFORMATION	A health care provider, health plan, employer, health or life insurer, school, or university must permit an individual to inspect and copy his/her PHI pertaining to that individual <i>unless</i> such information: (1) could reasonably be expected to <i>endanger the life or physical safety of</i> , or <i>cause substantial mental harm to</i> , any individual; (2) could reasonably lead to the identification of a <i>confidential source</i> of PHI; (3) is compiled principally for use in <i>litigation</i> ; or (4) was collected for unfinished, IRB-approved <i>clinical research</i> purposes. If an entity denies an individual access to PHI, the entity must inform the individual of the <i>reasons</i> for denial, any <i>procedures</i> for further review, and the individual's <i>right to file</i> a statement regarding the request. (pp. 19-23)	A health care provider, health researcher, health plan, employer, health or life insurer, school, or university <i>must permit an individual to inspect and copy</i> PHI pertaining to that individual. (pp. 18-19)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
AMENDMENT OF PROTECTED HEALTH INFORMATION	Within 45 days of receiving a request to amend information from an individual, a health care provider, health plan, employer, health or life insurer, school, or university must <i>make and notify</i> the individual of the amendment and <i>make reasonable efforts to inform</i> others previously receiving such information of any nontechnical amendments. If an entity refuses to make the amendment, the entity must inform the individual of the <i>reasons</i> for refusal, any <i>procedures</i> for further review, and the individual's <i>right to file</i> a statement of disagreement. (pp. 23-25)	The same, except <i>health researchers</i> are also covered. (pp. 19-21)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
NOTICE OF CONFIDENTIAL PRACTICES	A health care provider, health plan, or health oversight agency, public health authority, employer, health or life insurer, health researcher, school, or university must <i>post or provide</i> notice of the entity's <i>confidentiality practices</i>, which must include: (1) a <i>description of an individual's rights</i> with respect to PHI; (2) the <i>uses and disclosures</i> of PHI authorized by federal law; (3) the <i>procedures for authorizing</i> and revoking disclosures; (4) the procedures established by the entity for the <i>exercise of the individual's rights</i>; and (5) the <i>right to obtain a copy</i> of the notice. A <i>model notice</i> is to be developed by the Secretary of Health and Human Services with the advice of the National Committee on Vital Health Statistics, derived from groups such as the <i>National Association of Insurance Commissioners and others</i>. Use of the model notice services as an absolute defense against claims of receiving improper notice. (pp. 26-27)	A health care provider, health plan, health oversight agency, public health authority, employer, health researcher, health or life insurer, school, or university must prepare written notice of the entity's <i>privacy practices</i>, which must include: (1) the <i>procedures for an individual to provide, object to, modify, and revoke authorization</i> to disclose PHI; (2) the <i>right to inspect, copy, and amend</i> PHI; (3) the <i>right not to have employment or the receipt of services conditioned</i> upon the execution of an authorization for disclosure; (4) a <i>description of employees who have access</i> to or use PHI within an entity; (5) a description of any <i>computerized information systems</i> used to store or transmit PHI, including a description of any links to other systems or databases outside the entity; (6) the <i>right to request segregation</i> of PHI, and to restrict the use of such information by employees, agents, and contractors of the entity; (7) the <i>uses and disclosures of PHI that do not require individual authorization</i>; and (8) a statement that an individual may <i>self-pay</i> for health care in order that no identifying information be disclosed to anyone other than the health care provider. A copy of the written notice of privacy practices <i>must be provided each time</i> authorization to disclose PHI is sought or upon request of an individual. A summary of the entity's privacy practices must be posted in a clear and conspicuous manner. <i>Model notice</i> is to be developed by the <i>Office of Health Information Privacy</i> (see below). (pp. 21-23)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
ESTABLISHMENT OF SAFEGUARDS	A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university must <i>develop safeguards</i> that are sufficient to protect the confidentiality, security, accuracy, and integrity of PHI. The Secretary of Health and Human Services must <i>promulgate regulations</i> under this section, after consultation with the National Committee on Vital Health Statistics. (p. 27)	The same entities are covered. The <i>Office of Privacy</i> (see below) must <i>promulgate model guidelines</i> to deal with uses of computer systems, access controls, audit trails, physical security, protection of remote access points and protection of external electronic communications, periodic security assessments, incident internal reports in sanctions, and such other systems developed through new technology. (p. 24-25)
ACCOUNTING FOR DISCLOSURES	A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university is required to <i>keep and maintain a record of any disclosures</i> that is <i>not made within the entity</i> in accordance with regulations promulgated by Health and Human Services. The entities are required to maintain a record of such disclosures for at least 7 years. An agent of an entity is required to maintain a record of disclosures made under the sections of the Act that allow limited disclosure without authorization. (pp. 32-33)	Same entities are required to <i>keep and maintain a record of any disclosures</i> that are not made for purposes of <i>payment or treatment</i> in accordance with regulations promulgated by the <i>Office of Privacy</i> . The entities are required to maintain a record of such disclosures for at least 7 years. An agent of an entity is required to maintain a record of disclosures made under the sections of the Act that allow limited disclosure without authorization. The entities are also required to <i>keep records of electronic attempts to access PHI</i> . (p. 25-26)
RULES REGARDING USE AND DISCLOSURE	A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university <i>may not disclose PHI except as specifically authorized under the provisions of this Act</i> . (p. 33)	Same. (p. 26)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
USE OR DISCLOSURE WITHIN AN ENTITY	A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university <i>may use or disclose</i> PHI within the entity without obtaining authorization if such activity is <i>compatible with and related to</i> the purposes for which the information was obtained. Agents of the entity are considered to be " <i>within the entity</i> ." (p. 34)	There is no special rule for disclosure "within an entity." To ensure that necessary disclosures within an entity occur for purposes of treatment and payment, two specific provisions are included. With regard to treatment, a provider <i>may condition</i> the provision of services upon receiving authorization disclosure of PHI <i>if</i> the provider believes the disclosure is necessary to avoid endangering the health or treatment of the individual. With regard to payment, if an individual refuses to provide an authorization necessary for billing, an entity can require that the individual self-pay (pp. 29 & 30)
SCOPE OF DISCLOSURE	Disclosure is <i>limited to information necessary to accomplish the purpose</i> for which the information is disclosed. Disclosed information must be labeled as PHI. This provision is repeated in sections dealing with (1) restriction of use and disclosure (sec. 201) (p. 34) and (2) authorization (secs. 203) (p. 43).	Same, except the restriction is repeated in the following sections: (1) authorization (sec. 202) (p. 30); (2) emergency circumstances (sec. 211) (p. 35); (3) protection and advocacy systems (sec. 213) (pp. 37-38); (4) oversight (sec. 214) (p. 39-40); (5) law enforcement (sec. 215) (pp. 43-44); (6) next of kin and directory information section (sec. 221) (p. 48); and (7) judicial and administrative (sec. 223) (p. 56).
CREATION OF NON-IDENTIFIABLE HEALTH INFORMATION	A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university <i>may disclose</i> PHI to another entity <i>for the purpose of creating non-identifiable information</i> , if the entity or its agent prohibits the use or disclosure of the information for purposes other than the sole purpose of creating non-identifiable information specified by the entity. (p. 35)	There is no special section for the creation of non-identifiable health information.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
DISCLOSURE USING THE KEY	Disclosure of a key, which is a method or procedure for using non-identifiable health information to identify an individual, or manipulation of a non-identifiable database to identify an individual, is a prohibited disclosure of PHI. (p. 35)	There is no special section for the disclosure of a key to non-identifiable health information.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
AUTHORIZATION FOR DISCLOSURE	Treatment, Payment, and Health Care Operations: Every employer offering a health plan, and every health plan offering enrollment to individuals or non-employer groups, must, as a <i>condition of enrollment</i>, obtain a <i>valid authorization</i> concerning the use and disclosure of PHI from each participant in the plan. A provider providing care to a person outside of that individual's network plan, or a provider providing care to an uninsured individual, must also obtain similar authorization. Based on the title of this section, it appears this authorization is for treatment, payment, and health care operations. (See p. 7 for broad definition of health care operations). A <i>health plan may terminate coverage</i> of an enrollee who has revoked his/her authorization if the plan determines that the revocation <i>resulted in the inability of the plan to provide appropriate care or conduct essential health care operations</i>. An individual may not bring an action against a person for disclosures made in <i>good faith</i> reliance on the individual's authorization at the time of disclosure. (pp. 36-38) Other Than for Payment, Treatment, or [Health Care Operations]³: A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university <i>may disclose</i> PHI for a purpose other than treatment, payment, or [health care operations] <i>only if</i> the individual who is the subject of the information provides a <i>valid authorization</i> independent of an authorization for treatment, payment, or health care operations. An entity <i>may not</i> condition the delivery of treatment or payment for services on the receipt of these authorizations.(pp. 40-41)	A health care provider, health plan, health oversight agency, public health authority, employer, health researcher, health or life insurer, school, or university <i>may disclose</i> PHI pursuant to a <i>written authorization</i> by the individual who is the subject. The delivery of payment for services <i>may not be conditioned</i> upon receiving such an authorization <i>nor may it be conditioned</i> upon receiving an authorization to link PHI with computerized formats of another entity. Treatment <i>may be conditioned</i> on an authorization for disclosure if a health care provider believes that such disclosure is <i>necessary so as not to endanger the health or treatment</i> of the individual. (pp. 27 & 29-30)

³The draft actually uses the term "Plan Administration," which has been replaced in other sections with "Health Care Operations." For the purposes of this side by side, we assume the inclusion of "Plan Administration" in this section was a typographical error.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
MODEL AUTHORIZATIONS	<i>Model authorizations</i> must be developed by the Secretary of Health and Human Services with advice from the National Committee on Vital Health Statistics. (p 43)	The Secretary of Health and Human Services must develop <i>model written authorization and limitations on authorizations</i> . (p. 30)
REQUIREMENTS FOR INDIVIDUAL AUTHORIZATION	To be valid, an authorization must: (1) identify the individual involved; (2) describe the nature of the health care information to be disclosed; (3) identify the type of person to whom the information is to be disclosed; (4) describe the purpose of the disclosure; (5) be subject to revocation by the individual; (6) be either in writing, dated, and signed by the individual; or in electronic form, dated and authenticated by the individual. (p. 38)	The same, plus the authorization must: (7) permit an individual to indicate that a particular person or entity is not authorized to receive the PHI; (8) provide the means by which an individual can indicate that some of the individual's PHI should be segregated; (9) permit an individual to indicate that PHI must not be transmitted outside the entity in a computerized, digital, optical, or other electronic format. (pp. 27-28)
SEGREGATION OF FILES	There is no special section addressing the segregation of files.	A health care provider, health researcher, health plan, health oversight agency, public health authority, employer, health or life insurer, law enforcement official, school, and university <i>must comply</i> with the request of an individual to segregate any PHI, other than administrative billing information, held by the entity; limit the use or disclosure of segregated information to those persons specifically designated by the subject of the PHI; and maintain such information outside of any computerized or electronic system. (pp. 31-32)
REVOCATION OF AUTHORIZATION	Revocation of authorization may be made at any time, <i>unless</i> the disclosure is required to effectuate payment. Authorization is deemed to be revoked at the time of plan cancellation or nonrenewal of a health plan, except as necessary to complete plan administrative and payment requirements. (pp. 38-40 & 41)	Same. (pp. 32-33)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
CORONERS AND MEDICAL EXAMINERS	A health care provider, health plan, health oversight agency, public health authority, employer, health or life insurer, health researcher, law enforcement official, school, or university <i>must provide</i> PHI to the coroner or medical examiner when needed to inquire into and determine the cause, manner, and circumstances of a death. (pp. 41-43)	There is no special section on coroners or medical examiners.
NEXT OF KIN	A health care provider, or a person who receives PHI <i>under emergency circumstances</i> (see below), <i>may disclose</i> PHI to an individual's next of kin, or to another person whom the individual has identified, if the individual has been notified of the <i>right to object</i> to such disclosure (unless the individual is not competent to object and there are no prior indications that such an objection would have been made); the PHI <i>relates to health care currently being provided</i> ; or the disclosure <i>is consistent with good medical or professional practice</i> . (p. 43-44)	Same, except there is no "consistent with good medical or professional practice" provision. (pp. 44-45)
DIRECTORY INFORMATION	A health care provider, or a person who receives PHI <i>under emergency circumstances</i> (see below), <i>may disclose</i> to any person an individual's <i>name, general health status, and location</i> on the premises if the individual has been notified of the <i>right to object</i> to such disclosure (unless the individual is not competent to object and there are no prior indications that such an objection would have been made). The individual, however, must give <i>express authorization</i> for disclosure if it would <i>reveal specific information</i> about the individual's condition or <i>put the individual at risk of harm</i> . (pp. 44-46)	Same. (pp. 45-46)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
RIGHTS OF MINORS	Individuals who are <i>18 years or older</i> may exercise their rights to inspect, amend, and disclosure of PHI. Individuals who are <i>under 14 years</i> old will have their rights exercised by their parents or legal guardians. Individuals who are <i>14-18 years</i> old, and who live in states in which they are permitted to obtain types of health care while acting alone may exercise their rights regarding their PHI under this Act with regard to that health care; conversely, individuals who are <i>14-18 years</i> and in states in which they are not allowed to act alone in receiving certain types of health care, they may not exercise such rights with regard to such health care. (pp. 46-47)	The same, except the age range is 14-17. (pp. 46-47)
EMERGENCY CIRCUMSTANCES	Disclosures of PHI are permitted without an individual's consent in cases where the disclosure is <i>necessary</i> to protect the <i>health or safety</i> of the individual who is the subject of the information from <i>serious, imminent harm</i>. No disclosure made in a <i>good faith belief</i> that the disclosure was necessary will be a violation under the Act. (pp. 47-48)	Disclosures of PHI to a health care practitioner, health care facility, law enforcement authority, or emergency medical personnel are permitted in order to allay or remedy a <i>threat of imminent physical or mental harm</i> to an individual who is the subject of such information. (pp. 34-35) In the event of a threat of harm to an individual <i>other</i> than the individual who is the subject of the information, any person may disclose PHI if there is an <i>identifiable threat of serious injury or death</i> to an identifiable individual or group of individuals; the subject of such information has the ability to carry out such a threat; and the release of such information is necessary to prevent or significantly reduce the possibility of such a threat.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
OVERSIGHT	A health care provider, health plan, health researcher, employer, health or life insurer, law enforcement official, school, or university <i>may disclose</i> PHI to a health oversight agency, an accrediting body, a public health authority, or a State insurance department for oversight purposes authorized by law. The oversight supervisor must provide the entity with a statement that the PHI is being sought for a legally authorized oversight function. The PHI obtained about an individual <i>may not be used in a legal action or investigation directed against the individual unless</i> such action arises out of or is directly related to the payment of health care or a claim of fraud. (pp. 48-49)	A health care provider, health researcher, health plan, public health authority, employer, health or life insurer, law enforcement official, school, or university <i>may disclose</i> PHI to a health oversight agency for oversight purposes authorized by law if the agency does not record identifying information of the individual who is the subject of such information, and it does not remove PHI from the premises, custody, or control of the entity possessing such information. The PHI obtained about an individual <i>may not be used in a legal action or investigation directed against the individual.</i> (pp. 38-40)
PUBLIC HEALTH	A health care provider, health plan, public health authority, employer, health or life insurer, law enforcement official, school, or university <i>may disclose</i> PHI to a public health authority for use in a legally authorized disease or injury report, public health surveillance, or public health investigation or intervention. (pp. 49-50)	A health care provider, health plan, public health authority, health researcher, employer, health or life insurer, law enforcement official, school, or university <i>may disclose</i> PHI to a public health authority when there is a <i>specific nexus between an individual's identity and a threat of a specific disease, death, or injury</i> to any individual or the public health; and the identity would allow public health officials to <i>prevent or significantly reduce the possibility</i> of such a threat. An entity, however, will not be liable for disclosure to a public health authority based upon a <i>good faith belief</i> that such information was required to protect an individual or the public health from a threat or was made pursuant Federal or state laws. (pp. 36-37)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
PROTECTION AND ADVOCACY SYSTEMS	There is no special provision included for protection and advocacy systems.	Disclosures of PHI to agencies charged by law to protect the health and safety of individuals with disabilities are permitted if the agency can establish that there is <i>probable cause to believe</i> that an individual who is the subject of such information is vulnerable to abuse or neglect by an entity providing health or social services to such individual. (pp. 37-38)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
HEALTH RESEARCH	A health care provider, health plan, public health authority, employer, health or life insurer, school, or university <i>may disclose</i> PHI to a health researcher only if [such entity]⁴ has in place (1) the policy required by the Secretary to assure confidentiality and appropriate use of PHI; (2) that policy is consistent with both <i>Federal Policy for the Protection of Human Subjects</i> (these informed consent rules allow a waiver of consent requirements in some circumstances) and the confidentiality criteria of the Food and Drug Administration; (3) the policy is referenced in every contract, memorandum for IRB approval, and informed consent authorization; (4) the project has been approved by an IRB; and (5) informed consent has been obtained or waived in accordance with the common rule. The recipient of PHI must destroy the identifiable information when not required for the project unless an <i>IRB</i> has determined a need to retain the identifiers and there is an adequate plan to protect the identifiers from disclosure. The information may be used only for research purposes as authorized by the individual. The Secretary of Health and Human Services must, with advice from the National Committee on Vital Human Statistics, develop <i>model language</i> for research. (pp. 50-55)	A health researcher must comply with the existing consent rules regarding disclosure of health information under the <i>Federal Policy for the Protection of Human Subjects</i> (these informed consent rules allow a waiver of consent requirements in some circumstances). The recipient of the PHI must destroy the identifiable information when not required for the project unless an <i>IRB</i> has determined a need to retain the identifiers and there is an adequate plan to protect the identifiers from disclosure. The information may be used only for research purposes as authorized by the individual. The Secretary of Health and Human Services must issue a <i>report</i> not later than one year after the enactment to determine if informed consent, beyond that required by the current federal policy, should be mandated. (pp. 48-52)

⁴ As drafted, the bill requires that a health care provider, health plan, public health authority, employer, health or life insurer, school, or university have in place a policy required by the Secretary to assure confidentiality of PHI. We assume the drafters meant to say if the *researcher* has in place such a policy.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
STUDY BY IOM	This Act commissions a study by the Institute of Medicine to be presented within 2 years to examine research issues, including IRBs. (pp. 89-90)	Not included.
DISCLOSURE IN CIVIL, JUDICIAL, AND ADMINISTRATIVE PROCEDURES	A health care provider, health plan, public health authority, employer, health or life insurer, law enforcement official, school, or university <i>may disclose</i> PHI pursuant to a <i>discovery request or subpoena</i> in a civil action or administrative proceeding or such a request made through a court order. A court is <i>required to issue</i> an order to disclose PHI <i>if</i> it determines that without a disclosure of such information the person requesting the order would <i>be impaired from establishing a claim or defense</i>. (p. 56) The order must provide that the information is <i>subject to court protection; specify to whom the information may be disclosed; specify that the information may not be otherwise disclosed or used; and meet other court determined requirements</i>. This provision does not apply to non-identifiable health information or to health information related to a party to the litigation whose medical condition is at issue. This section does not supersede any grounds that may apply under Federal or State law for objecting to the disclosure of PHI. (pp. 56-57)	A health care provider, health plan, health oversight agency, employer, health or life insurer, school or university, or person who receives PHI under emergency circumstances <i>may disclose</i> PHI: (1) in connection with litigation or proceedings in which the individual who is the subject of the information has placed his or her <i>physical or mental condition at issue</i>, and such disclosure is made pursuant to the standards and procedures in the Federal Rules of Civil or Criminal Procedure or comparable rules of other courts or agencies; (2) to a court and to others ordered by the court when a court order has been issued; (3) if necessary to present a court an application regarding the provision of treatment to an individual or the appointment of a guardian; or (4) pursuant to a law requiring the reporting of specific medical information to law enforcement authorities. A court order may only be issued if the person seeking disclosure demonstrates by <i>clear and convincing evidence</i> that the information is <i>necessary for the adjudication of a material fact</i> in dispute, the need cannot be satisfied by non-identified information, and the need outweighs the individual's privacy concerns. The individual whose PHI is requested must be notified of the request. (pp. 52-56)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
LAW ENFORCEMENT	A health care provider, health plan, health oversight agency, employer, health or life insurer, school, or university <i>may disclose</i> PHI if done pursuant to a grand jury, administrative, or judicial subpoena, judicial warrant, <i>or any other lawfully authorized request</i> from a law enforcement agency. Once the matter has concluded the information must be destroyed or returned to the person from whom it was obtained. If the PHI is obtained without meeting these requirements, the information must be <i>excluded as evidence</i> .(p. 57-59)	A health care provider, health researcher, health plan, health oversight agency, employer, health or life insurer, school, university, court, or person who receives PHI under emergency circumstances <i>may disclose</i> PHI to a law enforcement authority <i>if</i> the disclosure is pursuant to a court order. A law enforcement authority may not obtain PHI unless the authority demonstrates by <i>clear and convincing</i> evidence that the information is <i>necessary to a legitimate law enforcement inquiry</i> into a particular violation of criminal law being conducted by the authority, <i>the need cannot be met using non-identifiable health information, and the need outweighs the privacy interests of the individual</i> . Unless the individual cannot be located or notification would risk the destruction of the evidence, the individual whose information is requested must be notified. Disclosure is limited to actions or investigations arising out of, or directly related to, the inquiry for which the information was obtained. (pp. 40-44)
PAYMENT CARE AND ELECTRONIC PAYMENT TRANSACTIONS	If an individual pays for health care using a <i>debit, credit, or other payment card or electronic</i> means, the entity receiving the payment may disclose to the issuer of the card or a processor only the PHI necessary for processing, billing, or collecting the payment. (p. 59-60)	There is no special section on electronic payments .
ELECTRONIC DISCLOSURES	The Secretary of Health and Human Services must promulgate <i>standards</i> for disclosing, authorizing, and authenticating PHI in electronic form. (p. 60)	Not included.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
INDIVIDUAL REPRESENTATIVES	An individual who is legally authorized to act as a representative of an individual may exercise that individual's rights under this Act. If an individual is not legally incompetent, but <i>suffers from a medical condition that prevents him/her from acting knowingly or effectively</i> , the rights under this Act may be exercised: first, by a person who holds a health care power of attorney for the individual; second, by a person who is legally recognized as an agent for the person; third, by the next of kin; and fourth, by a health care provider. (p. 61-63)	Same. (pp. 56-58)
LIMITED LIABILITY FOR LAW ENFORCEMENT	Broad immunity provision for federal and state law enforcement officers: such officers are not liable for any violations of this Act <i>unless</i> the violation resulted from intentional conduct with the intent to <i>sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm</i> . (p. 63)	Not included.
TORT LIMITED LIABILITY	A health care provider, health plan, health oversight agency, employer, health or life insurer, school, or university is not liable, regardless of State tort common law, for valid disclosures that are permissible under this Act. (p. 63)	Not included.

TOPIC	Bennett/Jeffords	Leahy/Kennedy
CRIMINAL SANCTION	If a person <i>knowingly and intentionally</i> obtains or discloses PHI in violation of Title II (restricting the use and disclosure of PHI), the penalty must not be more than \$50,000, up to 1 year in prison, or both; if committed under <i>false pretenses</i> , not more than \$250,000, up to 5 years in prison, or both; if committed with <i>intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm</i> , not more than \$500,000, not more than 10 years in prison, exclusion from all federally funded health programs, or any combination. The penalties must be doubled for every subsequent conviction. (pp. 67-69)	Same. (pp. 60-62)
DEBARMENT	The Attorney General must promulgate regulations to establish procedures to permit debarment of health care providers, health researchers, health or life insurers, or schools, or universities for receiving benefits from Federal health programs if managers or officers are guilty of violating this Act, have civil penalties imposed against them, or guilty of making false statements or obstructing justice relating to concealing illegal disclosures. (pp. 69-71)	Same. (pp. 62-64)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
CIVIL SANCTION	A health care provider, health researcher, health oversight agency, public health agency, law enforcement officer, employer, health or life insurer, school, or university who has <i>substantially and materially failed to comply with this Act</i> will be subject to not more than \$500 for each title I violation (a violation of the provisions providing access to and amendment of one's own PHI), not to exceed \$5000 in the aggregate; \$10,000 for each title II violation (a violation of the prohibitions and limitations on the use and disclosure of PHI), not to exceed \$50,000 in the aggregate; and, if violations are found to occur with such frequency as to constitute a <i>general business practice</i> , then the penalty must be up to \$100,000. (pp. 72-83)	Same. (pp. 64-74)
CIVIL ACTION	An aggrieved individual whose rights under this Act were <i>knowingly or negligently violated</i> may bring a civil action to recover preliminary and equitable relief, and the greater of compensatory damages or \$5000 in liquidated damages. Prevailing individuals may receive reasonable attorney's fees and other litigation costs and expenses, including expert fees. (pp. 84-85)	An aggrieved individual may bring a civil action to recover preliminary and equitable relief, actual damages, the greater of actual damages or \$5000 in liquidated damages, punitive damages, and attorney's fees and other litigation costs and expenses, including expert fees, depending on whether the violation was a result of <i>negligent</i> conduct or <i>knowing</i> conduct. (pp. 74-75)
RELATIONSHIP TO OTHER LAWS	This Act <i>preempts</i> any State law that directly relates to matters covered by this Act. A limited number of state laws and regulations (regarding reporting of statistics, abuse and neglect, communicable diseases and the collection, analysis, dissemination of information for developing use, cost effectiveness, performance, or quality data) are retained. (pp. 85-86)	This act <i>does not preempt</i> Federal or State laws and regulations that provide protections for the rights of individuals to the privacy of, or access to, their health information that are greater than those provided in this Act. (pp. 75-76)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
REPORTS CONCERNING FEDERAL PRIVACY ACT	This Act requires each agency head in 1 year to assess this Act's impact on each agency, as well as concerns regarding the Federal Privacy Act. (p. 87)	The Act maintains the Federal Privacy Act. (p. 77)
APPLICATION TO CERTAIN FEDERAL AGENCIES	The Act leaves in place several federal laws that protect privacy, but at the same time <i>exempts</i> the Departments of Defense, Transportation, and Veterans Affairs from certain provisions of the Act. (pp. 88-89)	Not included.
OFFICE OF PRIVACY	Not included.	This Act establishes an <i>Office of Privacy</i> within the Department of Justice, to be headed by a director appointed by the Attorney General. The Director of the Office of Privacy is to provide for enforcement of the Act, investigate complaints of alleged violations of the Act, provide guidance to the Attorney General in the implementation of this Act, prepare and submit reports required by the Act, and carry out any other activities determined appropriate by the Attorney General. (pp. 59-60)

TOPIC	Bennett/Jeffords	Leahy/Kennedy
PROHIBITION AGAINST RETALIATION	Not included.	A health care provider, health researcher, health plan, health oversight agency, employer, health or life insurer, school, or university who receives PHI <i>under emergency circumstances may not adversely affect</i> another person, directly or indirectly, because such person has exercised his/her rights under this Act, discloses information regarding a violation of this Act, or assisted someone in exercising his/her rights under this Act. (pp. 58-59)
EFFECTIVE DATE AND REGULATIONS	Regulations must be issued by HHS 12 months after the enactment of the Act. The Act does not take effect until 12 months <i>after</i> the promulgation of regulations. If HHS has not issued regulations 18 months after the date of enactment, the Act takes effect 30 months after enactment, or 6 months after promulgation of regulations, whichever is earlier. (pp. 90-91)	Same. (p. 78)