Resolved, That the American Bar Association supports federal, state and territorial legislation that protects the confidentiality of personally identifiable health information in either paper or electronic form.

Further Resolved, That such legislation should include individual privacy protections that ensure:

1) that individuals have the right to see, copy, and correct their personally identifiable health information and to delegate this right to others;

2) that disclosure of personally identifiable health information is not permitted without written authorization by the individual who is the subject of the information, except for the most compelling, limited, specific purposes, such as compliance with a proper discovery request or subpoena in a civil action, or, in the case of a law enforcement investigation, in response to a court order issued pursuant to Fourth Amendment warrant requirements; and

3) that parties who violate the law are subject to meaningful civil and criminal penalties and that a person aggrieved by a violation of the law has a private right of action.

Further Resolved, That the American Bar Association encourages, in the absence of legislative mandate, the parallel development of a code of fair health information practices, and such code should promote the confidentiality and protection against misuse of personally identifiable health information.
Introduction

This proposed policy supports the passage of federal legislation to protect the privacy of personally identifiable health information. Such legislation should incorporate the fundamental fair information practice principles of providing individuals with access to their own records; requiring consent to disclosures, with few exceptions; providing strong enforcement mechanisms and severe penalties for violation of the law; and limiting law enforcement access.

A number of studies have concluded that federal legislation is needed to address the inadequacy and variability of state laws in this area. As the health information infrastructure is being developed, it is critical that privacy protections be in place so that information is not vulnerable to abuse and misuse. If individuals do not believe that their information will be protected, they will be reluctant to seek health care and fully divulge information to their doctors.

The Association's support of federal privacy legislation for personal health information is important to building consensus around federal legislation and creating a set of recommendations to guide the Congress in its consideration of legislative proposals.

Background

The societal impact of technological innovations, including those that allow medical records, data, and images to be transferred easily over great distances, is felt across our country in significant ways. The development of a national information infrastructure and information superhighway are changing the ways we deal with each other. Traditional barriers of distance, time, and location are disappearing as information and transactions become computerized, and few relationships in the health care field will remain unaffected by these changes. In the absence of any Congressional action, the collection and use of personally identifiable health information will continue to occur within electronic networked environments without privacy protections.

While the information revolution holds great promise for enhancing our nation’s health, personal health information, in both paper and electronic form, must be handled within enforceable privacy rules. Today only 28 states allow patients access to their own medical records, and 34 states have conflicting confidentiality laws. A number of federal studies have concluded that a federal law is needed to protect people's medical records. In 1994, the Office of Technology Assessment (OTA) issued a report entitled, Protecting Privacy in Computerized Medical Information, which addresses the effects of the computerization of medical records on people’s privacy. In recommending comprehensive federal legislation, OTA found that:

[The expanded use of medical records for non-treatment purposes exacerbates the shortcomings of existing legal schemes to protect privacy in patient information. The law must address the increase in the flow of data outward from the medical care relationship by both addressing the question of appropriate access to data and providing redress to those who have]
been wronged by privacy violations. Lack of such guidelines, and failure to make them enforceable, could affect the quality and integrity of the medical record itself. (OTA Report, p. 44).

The Institute of Medicine (IOM) of the National Academy of Science also has released a study that focused on the risks and opportunities associated with protecting the privacy and confidentiality of personally identifiable health data. The IOM report recommends that Congress enact legislation to establish a uniform requirement for the confidentiality and protection of privacy rights for personally identifiable health data and to specify a Code of Fair Health Information Practices to ensure a proper balance among the competing concerns required disclosures, use of data, and patient privacy.

These studies have recognized that unauthorized disclosure of personal health information can have disastrous consequences. In one instance, for example, a journalist disguised himself as a doctor, obtained an actress' medical record, and published a story that she had been treated for a sexually transmitted disease. In another case, a physician at a large New York City medical school logged on to a computer system, discovered that a nurse was pregnant, and publicized that information. A Colorado medical student sold medical records to attorneys practicing malpractice law. These are just a few of the more well known stories; undoubtedly there are millions of similar breaches that occur outside the media spotlight, and often without the knowledge of the individuals harmed.

Despite the public and private horror stories, however, many Americans trust that the information they share with their doctor is kept private. Indeed, the traditional nature of the doctor-patient relationship is intended to foster trust and to encourage full disclosure. However, once a patient's information is submitted to a third-party payor, or to any other entity, the ethical tie between doctor and patient evaporates. In a particularly telling statistic, 93% of those termed "leaders" in a recent survey, including hospital CEOs, health insurance CEOs, physicians, nurses, and state regulators, believe that third party payers need to be governed by detailed confidentiality and privacy policies.

Within our current health care system, some people try to protect themselves against potential privacy violations. They routinely ask doctors to record false diagnoses because they fear their employers may see their health records, or they may fail to tell their doctors everything about their medical conditions for fear of losing control over this sensitive information. In psychiatric practices, it is common for patients to ask doctors not to take notes during sessions for fear such notes could be leaked or even obtained legally with a subpoena. Some people try to avoid the creation of records altogether by paying for medical services out-of-pocket, even though they are entitled to insurance coverage.

No federal law prevents disclosures by insurers to employers. Most patients, of course, believe the fiduciary relationship is between themselves and their doctors and do not realize that a third party with no direct relationship to their medical treatment actually controls health information.
about them. It is intolerable to support a system in which an employer's payment of a portion of employees' health care premiums, a normal part of most American employees' compensation packages, amounts to employees' controlling their employees' health records.

The problems that arise because of a lack of uniform, federal privacy protection for identifiable health information are often exacerbated by advances in technology. For example, at the state and local level today, employers, insurers, and health care providers are forming coalitions to develop automated and linked health care systems containing lifetime health histories on millions of Americans. The primary goals of these projects are cost reduction and improved quality of care.

Attempts are being made in some states to address the privacy, confidentiality, and security of health data by crafting internal guidelines, regulations, and contracts. In addition, in those states where the automation of health care information is seen as a key component of a state's health care reform package, state legislators and public agencies are attempting to enact legislation that establishes a right of privacy in personally identifiable health care information. These states also are attempting to design effective enforcement penalties and oversight mechanisms to monitor the information practices of the newly created health care systems.

The outcome of this piecemeal, state-by-state approach to protecting the privacy and security of health care information will be conflict among the states and a setback for the overall goal of privacy protection. Relegating the protection of health care information to the states' different guidelines, policies, and laws leaves individuals subject to differing degrees of privacy depending upon where they receive their health care. In some instances, individuals travelling across county or state lines to receive necessary medical treatment may lose their ability to control how their personal medical information is used. Moreover, states and local governments with different rules governing the use of health care information may be prevented from sharing health care information contained in their systems with neighboring states that do not have sufficient privacy protections.

To remedy the current problems in the health information system and to help build in privacy protections into the emerging electronic information systems, the proposed recommendation supports federal legislation containing the following principles:

1) that individuals have the right to see, copy, and correct their personally identifiable health information; 2) that disclosure of personally identifiable health information is not permitted without authorization by the individual who is the subject of the information, except for limited specific purposes, such as emergency medical circumstances, compliance with public health mandates and appropriate government oversight functions, or, in the case of a law enforcement investigation, in response to a court order issued pursuant to Fourth Amendment warrant requirements; and 3) that parties who violate the law are subject to meaningful civil and criminal penalties and that a person aggrieved by a violation of the law has a private right of action.
To avoid abuse, disclosure made pursuant to a need for government oversight should be limited by requiring oversight officials to obtain an administrative summons or subpoena for access to identifiable records. Additionally, health oversight agencies should not be permitted to re-disclose identifiable information for other purposes not specially authorized. Finally, a health oversight agency may not use the information gathered in its oversight role for any actions against an individual other than those arising out of receipt or payment for health care or fraud. With the inclusion of a legal process for access to identifiable information, the legislation can strike a fair balance between individual privacy and the government's legitimate needs to conduct audits and control fraud.

CONCLUSION

The protection of personally identifiable health information is critical to ensuring public trust and confidence in the emerging health information infrastructure. Health care reform cannot move forward without assuring the American public that the highly sensitive personal information contained in their medical records will be protected from abuse and misuse. If people are expected to embrace and participate in health reform environment, the price of their participation must not be the loss of control of sensitive personal information. In the end, any system that fails to win the public's trust will fail to win the public's support, and this country risks having individuals withdraw from full and honest participation in their own health care.

Respectfully submitted,

Abby R. Rubenfeld
Chair, Section of Individual Rights and Responsibilities

February 1996
1. **Summary of Recommendation(s).**

This recommendation supports the enactment of federal legislation to protect the privacy of personally identifiable health information by ensuring that individuals have access to their own records, that disclosures of such information generally are subject to the individual's consent, that law enforcement agencies have access to information only in accordance with Fourth Amendment principles, and that strong enforcement mechanisms and severe penalties are in place to address violations of the law.

2. **Approval by Submitting Entity.**

The Section Council approved the resolution and report in principle at its Oct. 20-21, 1995, meeting in Nashville, Tenn. The Executive Committee approved the final submission by telephone poll on Nov. 20, 1995.

3. **Has this or a similar recommendation been submitted to the House or Board previously?**

No.

4. **What existing Association policies are relevant to this recommendation and how would they be affected by its adoption?**

Over the last 25 years, the ABA has adopted numerous policies relating to privacy and to the confidentiality of records other than medical records. In 1975, for example, the ABA adopted a broad policy supporting various principles to protect the privacy of personal records kept by the government or by organizations. Other ABA policies involving privacy rights include a 1975 resolution supporting amendments to the Banking Secrecy Act that would ensure the confidentiality of financial records without hindering law enforcement investigations. A second 1975 policy supports legislation to facilitate and regulate the exchange of criminal justice information to protect against unauthorized use and ensure privacy. In addition, the ABA adopted a 1980 policy addressing Federal Bureau of Investigation access to records involving individuals; a 1983 resolution endorsing amendments to the Freedom of Information Act, including one that would extend FOIA exemptions involving personal information; a 1986 resolution supporting amendment of the Privacy Act of 1974 and other statutes to enhance

---

**GENERAL INFORMATION FORM**

Submitting Entity: Section of Individual Rights and Responsibilities

Submitted By: Abby Rubinfeld, Chair
privacy and guarantee fair information practices by government agencies; and a 1986 
resolution supporting amendments to the federal wiretap law to safeguard the transmission of 
all forms of information, including voice, data, and video. In addition, the ABA has adopted 
comprehensive policies relating to health records of persons with HIV/AIDS (1988-1990) and 
persons with mental disabilities (1978). The proposed resolution would build upon and update 
the privacy principles adopted in 1979 by addressing their applicability in the specific context of 
medical records maintained in computer databases, as well as paper files.

5. What urgency exists which requires action at this meeting of the House?

On October 24, 1995, Senator Robert F. Bennett (R-UT) introduced the "Medical Record 
Confidentiality Act of 1995" (S. 1360), designed to establish a mechanism to protect the 
confidentiality of personally identifiable health care information. This legislation, which 
addresses many of the issues covered in this Report with Recommendation, is likely to come 
up for consideration by the full Congress early in the 1996 session.

6. Status of Legislation. (If applicable.)

The Senate Labor and Human Resources Committee held a hearing on S. 1360 on Nov. 14, 
1995.

7. Cost to the Association. (Both direct and indirect costs.)

Adoption of the recommendation would result only in minor, indirect costs of Governmental 
Affairs and Section staff time devoted to policy dissemination and implementation as part of 
staff members' overall substantive responsibilities.

8. Disclosure of interest. (If applicable.)

Janeti Goldman, a primary author of the draft report, is a privacy rights advocate with the 
Center for Democracy and Technology, which generally supports S. 1360 with some changes.

9. Referrals.

Referrals of this report are being made in accordance with Rule 45.7(b). In addition, the 
Section is distributing a memorandum outlining the substance of the report with 
recommendation to the following ABA entities that may have a specific interest in the subject 
matter:
Sections, Divisions, and Forums

Administrative Law and Regulatory Practice
Business Law
Criminal Justice
Family Law
General Practice
Government and Public Sector Lawyers
Intellectual Property
Labor and Employment Law
Law Student
Litigation
Science and Technology
Senior Lawyers
State and Local Government Law
Tort and Insurance Practice
Young Lawyers
Health Law

Special Committees and Commissions

Coordinating Group on Bioethics and the Law
Commission on Domestic Violence
Commission on Homelessness and Poverty
Coordinating Committee on Immigration Law
Commission on Legal Problems of the Elderly
Medical Professional Liability
Commission on Mental and Physical Disability Law

10. Contact Person(s). (Prior to the meeting)

Janet Goldman (Chair, IPR Section's Privacy Committee)
Center for Democracy and Technology
1001 G Street, NW, Suite 700 East
Washington, DC 20001
(202) 637-0800
11. Contact Person. (Who will present the report to the House)

Robert F. Drinan, SJ (Section Delegate)
Georgetown University Law Center
600 New Jersey Avenue
Washington, DC 20001
(202) 662-9412

12. Contact Person Regarding Amendments to This Recommendation. (Are there any known proposed amendments at this time? If so, please provide the name, address, telephone, fax and ABA/Net number of the person to contact below.)

None known at this time.