Recommendations from Past Reports: *Privacy*

Recommendation	Report	Implemented?
There must be no personal data record keeping systems whose very existence is secret.	*Records, Computers and the Rights of the Citizens* (1973)	
There must be a way for an individual to find out what information about him is in a record and how it is used.	*Records, Computers and the Rights of the Citizens* (1973)	
There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.	*Records, Computers and the Rights of the Citizens* (1973)	
There must be a way for an individual to correct or amend a record of identifiable information about him.	*Records, Computers and the Rights of the Citizens* (1973)	
Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.	*Records, Computers and the Rights of the Citizens* (1973)	
We recommend the enactment of legislation establishing a Code of Fair Information practice for all automated personal data systems. • The Code should define "fair information practice" as adherence to specified safeguard requirements. • The Code should prohibit violation of any safeguard requirement as an "unfair information practice." • The Code should provide that an unfair information practice be subject to both civil and criminal penalties. • The Code should provide for injunctions to prevent violation of any safeguard requirement. • The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits.	*Records, Computers and the Rights of the Citizens* (1973)	

Recommendations	Report	Implemented?
In light of our inquiry into the statistical-reporting and research for uses of personal data in administrative record-keeping systems, we recommend that steps be taken to assure that all such uses are carried out in accordance with five principles: **First,** when personal data are collected for administrative purposes, individuals should under no circumstances be coerced into providing additional personal data that are to be used exclusively for statistical reporting and research. When application forms or other means of collecting personal data for an administrative data system are designed, the mandatory or voluntary character of an individual's responses should be made clear. **Second,** personal data used for making determinations about an individual's character, qualifications, rights, benefits, or opportunities, and personal data collected and used for statistical reporting and research, should be processed and stored separately. **Third,** the amount of supplementary statistical-reporting and research data collected and stored in personally identifiable form should be kept to a minimum. **Fourth,** proposals to use administrative records for statistical reporting and research should be subjected to careful scrutiny by persons of strong statistical and research competence. **Fifth,** any published findings or reports that result from secondary statistical-reporting and research uses of administrative personal data systems should meet the highest standards of error measurement and documentation.	*Records, Computers and the Rights of the Citizens* (1973)	

Recommendations	Report	Implemented?
We recommend that all personal data in such systems be protected by statute from compulsory disclosure in identifiable form. Federal legislation protecting against compulsory disclosure should include the following features: • The data to be protected should be limited to those *used exclusively for statistical reporting or research.* Thus, the protection would apply to statistical-reporting and research data derived from administrative records, and kept apart from them, but not to the administrative records themselves. • The protection should be limited to data *identifiable with, or traceable to, specific individuals.* When data are released in statistical form, reasonable precautions to protect against "statistical' disclosure" should be considered to fulfill the obligation not to disclose data that can be traced to specific individuals. • The protection should be specific enough to qualify for non-disclosure under the Freedom of Information Act exemption for matters "specifically exempted from disclosure by statute." 5 U.S.C. 552(b)(3). • The protection should be available for data in the custody of all statistical-reporting and research systems, whether supported by Federal funds or not. • Either the data custodian or the individual about whom data are sought by legal process should be able to invoke the protection, but only the individual should be able to waive it. • The Federal law should be controlling; no State statute should be taken to interfere with the protection it provides.	*Records, Computers and the Rights of the Citizens* (1973)	

Recommendations	Report	Implemented?

Recommendations	Report	Implemented?
We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government and government-supported automated personal data systems.	*Records, Computers and the Rights of the Citizens* (1973)	
As a general framework for action on the Social Security number, we recommend that Federal policy with respect to use of the SSN be governed by the following principles: **First,** uses of the SSN should be limited to those necessary for carrying out requirements imposed by the Federal government. **Second,** Federal agencies and departments should not require or promote use of the SSN except to the extent that, they have a specific legislative mandate from the Congress to do so. **Third,** the Congress should be sparing in mandating use of the SSN, and should do so only after full and careful consideration preceded by well advertised hearings that elicit substantial public participation. Such consideration should weigh carefully the pros and cons of any proposed use, and should pay particular attention to whether effective safeguards have been applied to automated personal data systems that would be affected by the proposed use of the SSN. (Ideally, Congress should review all present Federal requirements for use of the SSN and determine whether these existing requirements should be continued, repealed, or modified.) **Fourth,** when the SSN is used in instances that do not conform to the three foregoing principles, no individual should be coerced into providing his SSN, nor should his SSN be used without his consent. **Fifth,** an individual should be fully and fairly	*Records, Computers and the Rights of the Citizens* (1973)	

Recommendations	Report	Implemented?
informed of his rights and responsibilities relative to uses of the SSN, including the right to disclose his SSN whenever he deems it in his interest to do so.		
We recommend specific, preemptive, Federal legislation providing: (1) That an individual has a legal right to refuse to disclose his SSN to any person or organization that does not have specific authority provided by Federal statute to request it; (2) That an individual has the right to redress if his lawful refusal to disclose his SSN results in the denial of a benefit, or the threat of denial of a benefit; and that, should an individual under threat of loss of benefits supply his SSN under protest to an unauthorized requestor, he shall not be considered to have forfeited his right to redress; and (3) That any oral or written request made to an individual for his SSN must be accompanied by a clear statement indicating whether or not compliance with the request is required by Federal statute, and, if so, citing the specific legal requirement. In addition, we recommend (4) That the Social Security Administration undertake a positive program of issuing SSNs to ninth-grade students in schools, provided (a) that no school system be induced to cooperate in such a program contrary to its preference; and (b) that any person shall have the right to refuse to be issued an SSN in connection with such a program, and such right of refusal shall be available both to the student and to his parents or guardians;	*Records, Computers and the Rights of the Citizens* (1973)	
The individual's right to control, use, and access his health care records, while obtaining requisite services and benefits, requires further consideration.	*Medical Records: Problems of Confidentiality and Privacy* (1978)	

Recommendations	Report	Implemented?
The committee recommends that the U.S. Congress move to enact preemptive legislation that will: • establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for person-identifiable health data and specify a Code of Fair Health Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy; • impose penalties for violations of the act, including civil damages, equitable remedies, and attorney's fees where appropriate; • provide for enforcement by the government and permit private aggrieved parties to sue; • establish that compliance with the act's requirements would be a defense to legal actions based on charges of improper disclosure; and • exempt health database organizations from public health reporting laws and compulsory process with respect to person-identifiable health data except for compulsory process initiated by record subjects.	*Health Data in the Information Age* (1994)	

Recommendations	Report	Implemented?
The committee recommends that health database organizations establish a responsible administrative unit or board to promulgate and implement information policies concerning the acquisition and dissemination of information and establish whatever administrative mechanism is required to implement these policies. Such an administrative unit or board should: • promulgate and implement policies concerning data protection and analyses based on such data; • develop and implement policies that protect the confidentiality of all person-identifiable information, consistent with other policies of the organization and relevant state and federal law; • develop and disseminate educational materials for the general public that will describe in understandable terms the analyses and their interpretation of the rights and responsibilities of individuals and the protections accorded their data by the organization; • develop and implement security practices in the manual and automated data processing and storage systems of the organization; and • develop and implement a comprehensive employee training program that includes instruction concerning the protection of person-identifiable data.	*Health Data in the Information Age* (1994)	

Recommendations	Report	Implemented?
The committee recognizes that there must be release of patient-identified data related to the processing of health insurance claims. The committee recommends, however, that a health database organization *not* release person-identifiable information in any other circumstances *except* the following: • to other HDOs whose missions are compatible with and whose confidentiality and security protections are at least as stringent as their own; • to individuals for information about themselves; • to parents for information about a minor child except when such release is prohibited by law; • to legal representatives of incompetent patients for information about the patient; • to researchers with approval from their institution's properly constituted Institutional Review Board; • to licensed practitioners with a need to know when treating patients in life-threatening situations who are unable to consent at the time care is rendered; and • to licensed practitioners when treating patients in all other (non-life-threatening) situations, *but only with the informed consent of the patient.* Otherwise, the committee recommends that health database organizations not authorize access to, or release of, information on individuals with or without informed consent.	*Health Data in the Information Age* (1994)	
Organizations that collect, analyze, or disseminate health information should adopt a set of fair information practices similar to those contained in the federal Privacy Act of 1974.	*For the Record: Protecting Electronic Health Information* (1997)	

Recommendations	Report	Implemented?
The Department of Health and Human Services should work with the US Office of Consumer Affairs to determine appropriate ways to provide consumers with a visible, centralized point of contact regarding privacy issues (a privacy ombudsman).	*For the Record: Protecting Electronic Health Information* (1997)	
The committee recommends that the U.S. Congress move to enact preemptive legislation that will: • establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for person-identifiable health data and specify a Code of Fair *Health* Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy; • impose penalties for violations of the act, including civil damages, equitable remedies, and attorney's fees where appropriate; • provide for enforcement by the government and permit private aggrieved parties to sue; • establish that compliance with the act's requirements would be a defense to legal actions based on charges of improper disclosure; and exempt health database organizations from public health reporting laws and compulsory process with respect to person-identifiable health data except for compulsory process initiated by record subjects.	*Health Data in the Information Age* (1994)	

Recommendations	Report	Implemented?
The Department of Health and Human Services should conduct studies to determine the extent to which—and the conditions under which—users of health information need data containing patient identities.	*For the Record: Protecting Electronic Health Information* (1997)	
Government and the health care industry should take action to create the infrastructure necessary to support the privacy and security of electronic heath information.	*For the Record: Protecting Electronic Health Information* (1997)	
The Secretary of Health and Human Services should establish a standing health information subcommittee within the National Committee on Vital and Health Statistics to develop and update privacy and security standards for all users of health information. Membership should be drawn from existing organizations that represent the broad spectrum of users and subjects of health information	*For the Record: Protecting Electronic Health Information* (1997)	
The federal government should work with industry to promote and encourage an informed public debate to determine an appropriate balance between the privacy concerns of patients and the information needs of various users of health information.	*For the Record: Protecting Electronic Health Information* (1997)	
Congress should provide initial funding for the establishment of an organization for the health care industry to promote greater sharing of information about security threats, incidents, and solutions throughout the industry	*For the Record: Protecting Electronic Health Information* (1997)	

Recommendations	Report	Implemented?
The American Medical Informatics Association (AMIA) recommends the use of the SSN as the patient identifier at the present time. In addition, we recommend the addition of a self-check digit to the SSN to reduce errors of identification whenever the number is hand-entered by an operator. Other options for patient identifiers should be explored for the long haul.	*Standards for Medical Identifiers, Codes, and Messages Needed to Create an Efficient Computer-stored Medical Record (1994)*	
The federal government and other HIT proponents must specifically address the protections to privacy and confidentiality afforded by the Health Insurance Portability and Accountability Act (HIPAA) and continue to promote and enforce related standards and safeguards accordingly.	*Health Information Technology (HIT) Leadership Panel Final Report (2005)*	
Consumer and patient advocacy groups should promote policies that encourage the use of electronic technologies in healthcare organizations and by healthcare providers to improve the quality of services, to decrease rates of adverse effects, and to increase access to online/wireless health information and services for consumers, patients, and clients. They should advocate for privacy protections for consumers, patients, and clients when they exchange health information electronically and for equal access to technology and information by all population groups.	*Final Report NHII - Information for Health: A Strategy for Building the National Health Information Infrastructure* (2001)	