Order Code IB98002

Medical Records Confidentiality

Updated April 25, 2000

C. Stephen Redhead
Domestic Social Policy Division

Harold C. Relyea
Government and Finance Division

Gina Marie Stevens
American Law Division

CONTENTS

Medical Records Confidentiality

SUMMARY

The 1996 Health Insurance Portability and Accountability Act (HIPAA) required Congress to enact a federal privacy law by August 21, 1999, or else the Secretary of Health and Human Services (HHS) must issue final medical records privacy regulations by February 21, 2000. Pursuant to HIPAA, the Secretary made recommendations to Congress on September 11, 1997, on ways to protect individually identifiable information.

When Congress failed to enact health privacy legislation prior to the 1999 deadline, the Secretary promulgated draft regulations on November 3, allowing for a 60-day comment period prior to issuing final regulations.

President Clinton has called on Congress to continue to work on privacy legislation, noting that HHS's authority is limited and that Congress could produce legislation that would provide stronger authority.

The ability to ensure the privacy of health records increasingly is at risk due to several trends. These include the growing use of information technologies in health care, structural changes in the health care delivery and payment systems, and information gathered from genetic testing. These factors accentuate the fact that existing legal safeguards to protect patient confidentiality are limited. In particular, concerns are raised about the increasing number of parties involved in health care treatment, payment, and oversight who have routine access to personally identifiable health records.

The concept of a "code of fair information practices", which is embedded in the Privacy Act of 1974, remains fundamental to all proposals today for maintaining confidentiality of personal records. Fair information practices include, among others, establishing conditions for disclosure of personally identifiable information, providing individuals with access to records held and the right to make corrections through emendation, and enforcing penalties for noncompliance.

Consensus exists on the need to implement fair information practices for health records, but a number of unresolved issues remain. For example, HHS recommendations were criticized for allowing law enforcement officials to gain access to personally identifiable health records without additional safeguards beyond existing law. Finding the appropriate balance between access to health records for research purposes and individual privacy rights has been the subject of much debate. The relationship between state law and possibly a uniform national law is highly contentious. Establishing effective mechanisms for authorizing access to confidential health information has been a challenge.

Several comprehensive medical records confidentiality bills have been introduced. Disagreements on a number of issues frustrated attempts to mark up a Senate HELP Committee draft bill during the first session of the 106th Congress.

MOST RECENT DEVELOPMENTS

On November 3, 1999, as mandated under the 1996 Health Insurance Portability and Accountability Act (HIPAA), the Secretary of Health and Human Services (HHS) proposed regulations (64 Fed. Reg. 59917) to protect the privacy of individually identifiable health information maintained or transmitted in electronic form. The regulations cover health plans, health care providers, and clearinghouses (i.e., entities that facilitate and process the flow of information between providers and payers). Under the proposed rule, patients have the right to inspect and amend their medical records. Health plans and providers are also required to obtain a patient's voluntary consent to disclose information unless the disclosure is related to treating an individual or paying for her care. Covered entities that fail to comply with the regulations would be subject to civil and criminal penalties, but patients would not be given the right to sue for violations of the law.

HHS received more than 50,000 comments on the proposed regulations during the public comment period, which closed on February 17, 2000. The Secretary has not set a date for issuing a final rule. Privacy advocates have urged Congress to continue to work on passing comprehensive health privacy legislation, noting that the Secretary's authority under HIPAA is limited. For more information on the proposed rule, see CRS Report RS20500, Medical Records Privacy: Questions and Answers on the Proposed Federal Regulations.

BACKGROUND AND ANALYSIS

Individuals have traditionally relied upon the understanding that the physician-patient relationship is confidential. However, legally, the physician-patient confidentiality privilege is limited to courtroom situations where issues of disclosure may arise. Many disclosures of personally identifiable medical records are made expressly with the consent of the patient. Informed consent by the patient has traditionally been offered as the primary mechanism for limiting access to individually identifiable records. For example, insurance companies receive information based upon a consent form signed by the patient, which also allows the sharing of the same information with the Medical Information Bureau (MIB). The MIB is a nonprofit trade association of major insurance companies that collects information that can assist in detecting fraud or omissions in life, health, or disability insurance applications.

The patient's expectation that information supplied to a physician is confidential may no longer be realistic. A growing number of disclosures occur, without the express consent of the patient, to public health agencies, health researchers, fraud and abuse investigators, and law enforcement agencies. The broad nature of many consent forms, the willingness of most patients to sign whatever form is presented, and the potential growth of routine, secondary, non-authorized disclosures of patient information create a false sense of privacy for many individuals. Concerns are increasing that, if patients believe their records are not confidential, they will no longer provide physicians with information potentially important for effective treatment.

Scientific developments, stimulated in part by the Human Genome Project (HGP), have led to remarkable progress in genetics and better understanding of alterations in genes that are associated with diseases in humans. This, in turn, has been accompanied by extraordinary opportunities to diagnose, treat, and prevent diseases. However, these advances simultaneously raise a number of complex issues related to the acquisition, protection, and use of genetic information. Concerns have been raised that access to genetic information by third parties, such as insurance companies and employers, will increase the potential for discrimination and stigmatization based on this information.

Growth in the application of information technologies to all aspects of health care and structural changes in health care delivery and payment systems not only offer significant opportunities for providing improved health care at contained costs, but also increase the threats to patient privacy and medical records confidentiality. Examples include the use of electronic medical records for maintaining clinical information and use of telemedicine to provide remote access to physicians, medical equipment, and diagnostic facilities by underserved communities. As reported in a study by the National Research Council, "the health care industry spent an estimated $10 billion to $15 billion on information technology in 1996." (National Research Council, Computer Science and Telecommunications Board, *For the Record: Protecting Electronic Information.* Washington, DC: National Academy Press, 1997, p. 2.)

Major organizational changes in the health care industry also provide an impetus for expanding use of information technology. There is a greater need to integrate information provided by participating institutions that are part of managed care systems, as compared to fee-for-service providers. Managed care organizations collect vast amounts of data on the costs, processes, and outcomes associated with various diseases, conditions, and treatments. In this new environment, data must be coordinated from patient services delivered in different settings, such as hospitals, clinics, pharmacies, and physicians offices, so that care and payment can be provided efficiently. The result is a growing number of secondary and tertiary users of personal health information.

Rapidly increasing requirements for the collection, integration, analysis, and storage of health information results in the creation of large scale databases, the capability to link data from distributed databases, and the ability for more people in dispersed locations to access data. A variety of mechanisms, both technological and organizational, may be employed to ensure that unauthorized access does not occur and that sufficient audit trails are maintained for proper accountability. Technical measures can be employed to limit access to authorized users for specifically designated purposes. Encryption, the use of smart cards or other unique identifiers for authenticating users, access control software, firewalls to prevent external attacks, and physical security and disaster recovery procedures are all important elements in creating a technologically secure environment. Computerization also makes it possible to develop approaches for making data anonymous so that individuals cannot be identified. Management practices, including the establishment of strong privacy policies, education and training, and implementing effective sanctions for abuses can contribute substantially to maintaining confidentiality of medical records.

The 1996 Health Insurance Portability Act required the Secretary of Health and Human Services (HHS) to make recommendations to Congress on ways to protect personally identifiable health information and to establish penalties for wrongful disclosure of health care

transactions. HIPAA imposed a deadline of August 21, 1999, for Congress to enact comprehensive health privacy legislation. If Congress failed to act, then under HIPAA the Secretary was authorized to issue medical privacy regulations by February 21, 2000.

The implementation of the European Union Data Privacy Directive in October 1998 provides further impetus for congressional action in the 106th Congress. Article 25 of the Directive requires EU member states to enact laws that prohibit the transfer of personal data to non-EU countries that lack an "adequate level of protection." Determinations of adequacy are to be made by the European Commission. If a finding of inadequacy is made, EU member states must block transfers of personal data to that third country. The U.S. views with concern the prohibition on the transfer of data from EU member countries to third countries that do not provide adequate privacy protection, and is engaged in discussions with European Union nations to resolve any problems that could threaten data flow.

Federal and State Laws Governing Health Data Privacy

Privacy has long been an important value in American society. When drafting the Bill of Rights, the founding fathers gave constitutional recognition to privacy expectations. Since the late nineteenth century, various developments—not the least of which have been new, intrusive technologies—have contributed to more disparate understandings of the concept of privacy and infringements upon it. As threats to privacy appeared to become more widespread, Congress and the executive branch began to examine the situation. For example, the House Committee on Government Operations chartered a Special Subcommittee on Invasion of Privacy in 1965. In 1973, Secretary of Health, Education, and Welfare Elliot L. Richardson established an Advisory Committee on Automated Personal Data Systems. In its July 1973 final report, *Records, Computers, and the Rights of Citizens*, the Secretary's Advisory Committee recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems."

Federal Privacy Act of 1974

The concept of a code of fair information practices was embodied in the Privacy Act of 1974 (5 U.S.C. 552a) and remains fundamental to all proposals today for ensuring individuals' privacy and maintaining the confidentiality of personal records. For example, the Privacy Act, which applies only to federal government agencies:

- limits the ability of agencies to disclose personally identifiable information;
- prescribes requirements for individuals to have access to their records and make corrections of such information;
- requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;"
- requires agencies to specify their authority and purposes for collecting personally identifiable information from an individual;
- requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy,

relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;" and
- provides civil and criminal enforcement arrangements.

Among the records to which the Privacy Act is applicable are "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, *medical history*, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." (emphasis added) Virtually all executive branch establishments and entities are subject to the requirements of the statute, and its access and emendation procedures may be utilized by any United States citizen or alien lawfully admitted for permanent residence. Because the act does not apply to any entities beyond federal government agencies, it has limited application to personally identifiable medical records, which are primarily held and accessed by private organizations.

Other Federal Statutes Relating to Health Information Confidentiality

A major impetus for medical records privacy legislation is the absence of comprehensive federal law that protects the confidentiality of patient records in all settings. Other federal statutes that provide limited protections under specific circumstances are summarized below. These provisions generally cover narrowly defined venues in which protections are provided.

- The Balanced Budget Act of 1997 amended the Social Security Act (18 U.S.C. 1852) to require that Medicare+Choice organizations that maintain medical information about their enrollees establish safeguards for the privacy of personally identifiable enrollee information and provide access to such records and information to enrollees. Under 42 U.S.C. 241(d), the Secretary of Health and Human Services (HHS) may authorize persons engaged in biomedical, behavioral, clinical, or other research to protect the privacy of research subjects by withholding the subjects' names or other identifying characteristics from persons not connected with the research.

- The Controlled Substances Act (21 U.S.C. 872) allows the Attorney General to authorize persons engaged in drug abuse research to withhold the names and other identifying characteristics of research subjects.

- The Alcohol, Drug Abuse, and Mental Health Administration Reorganization Act amended the Comprehensive Alcohol Abuse & Alcoholism Prevention, Treatment & Rehabilitation Act of 1970 (42 U.S.C. 290dd-2) to make records of the identity, diagnosis, prognosis, or treatment of substance abuse patients confidential and require authorization for disclosure.

- The Veterans Benefits section of the *U.S. Code* provides for the confidentiality of medical records maintained in connection with programs or treatment related to drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia (38 U.S.C. 7332). Disclosures require written consent of the subject or must be expressly authorized in statute.

- The Public Health Service Act (42 U.S.C. 299a-1(c)) prohibits personally identifiable information from research, demonstration projects, and evaluation conducted or supported by the Agency for Health Care Policy and Research from being used, published, or released for any purpose other than the purpose for which it was supplied.

- The Americans with Disabilities Act of 1990 (42 U.S.C. 12112) provides some protection of health information for individuals with disabilities. It prohibits an employer, employment agency, labor organization, or joint labor-management committee from requiring a medical examination and inquiring whether an employee is disabled, unless the examination or inquiry is shown to be job-related and consistent with business necessity.

- The Social Security Act (42 U.S.C. 1306) prohibits disclosure of any return or portion of a return filed with the Commissioner of Internal Revenue under title VIII of the Social Security Act (42 U.S.C. 1001 *et seq.*) or under subchapter E of chapter 1 or subchapter A of chapter 9 of the Internal Revenue Code, unless otherwise provided by federal law or as prescribed by the head of the Social Security Administration (SSA) or the Department of Health and Human Services (HHS) by regulation.

However, other statutes expressly authorize access to personal information without prior written consent for such purposes as peer review and fraud investigations.

- The Inspector General Act of 1978 (5 U.S.C. 6) grants each Inspector General the authority to access all records, audits, reviews, documents, papers, recommendations, or other materials that relate to programs and operations for which the Inspector General has responsibilities, and also to subpoena documentary evidence necessary for the IG to perform the IG's functions.

- The Health Insurance Portability and Accountability Act, described below, also authorizes the Attorney General to issue a subpoena for health records when conducting a health care fraud investigation.

- The Social Security Act (42 U.S.C. 1320c-3) authorizes peer review organizations to examine pertinent records of any practitioner or provider of health care services and inspect facilities in which the care is rendered or services are provided as part of a review of the professional activities of physicians and other health care practitioners and institutional and noninstitutional health care service providers to evaluate the quality, reasonableness and/or medical necessity of services provided. The act prohibits disclosure of any data or information acquired by the organization in exercising its duties and functions to any person not specified in the exceptions.

HIPAA Provisions on Medical Records Privacy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191) included an Administrative Simplification title, which will require all health care providers, plans, and clearinghouses that use electronic health information to adhere to new federal standards for the electronic transmission and security of personal health data. Those standards include uniform formats and data codes for electronic billing and claims forms, security measures to protect personally identifiable health information, and unique identifiers (i.e., identification numbers) for health plans, providers, employers, and individuals. In enacting the Administrative Simplification provisions, Congress intended to streamline the processing of health care claims, reduce paperwork, lower costs, improve accuracy, safeguard the security of information, and facilitate networking and coordination of health care activities.

To date, the Secretary has issued proposed regulations for national standards for transactions and code sets, and security. Proposed standards for unique identifiers for employers and providers have also been issued. The proposed standard for a health plan identifier is still under development. However, development of a unique individual identifier has raised serious confidentiality and privacy concerns. HHS held the first of a series of planned regional public hearings in Chicago on July 20-21, 1998, which provoked a great deal of controversy. In July 1998, the Clinton Administration decided to delay the implementation of the unique health identifier until Congress enacts a privacy act . In addition, language in both the FY1999 and FY2000 appropriations bills prohibited the use of funds for adopting a unique health identifier for individuals until legislation is enacted specifically approving the standard.

In addition to the electronic data requirements, HIPAA also provided a timetable for taking action to protect the privacy of personally identifiable medical information. The law required the Secretary to make recommendations to Congress by August 1997 on ways to protect medical records privacy. The Secretary delivered her report at a hearing before the Senate Labor and Human Resources Committee on September 11, 1997. HIPPA gave Congress until August 21, 1999, to enact a privacy law. When Congress failed to meet that deadline, the Secretary, as required by HIPAA, issued a proposed health privacy rule on November 3, 1999. HIPAA states that the regulation may not supersede more protective state privacy laws. Additional information on the privacy and other Administrative Simplification regulations may be found at [http://aspe.os.dhhs.gov/admnsimp].

EU Directive

The 1995 European Union (EU) *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* (Data Privacy Directive at [http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html]) required that, by October 1998, all 15 EU member states make their national privacy laws consistent with the Directive. After that, the EU may limit flows of data between countries that do not have comparable protections for personally identifiable data. This prospect raises concerns among U.S. companies that, if the United States is deemed to have inadequate privacy protection in such a critical area as medical records, it could create barriers to the international exchange of information. The U.S. approach to privacy, which differs from that of the European Community, relies upon a sectoral approach based upon a combination of legislation,

regulation, and self regulation. Considerable efforts have been made recently to improve the credibility and enforceability of industry self regulation. Because of those differences in approach, many in the U.S. have expressed concern about the implementation of the EU "adequacy" standard on transfers of personal data from Europe.

To address this concern, the U.S. Department of Commerce has issued a set of "Draft International Safe Harbor Privacy Principles" for public comment [http://www.ita.doc.gov/ecom/menu.htm]. Industries that adhere to the principles would be allowed to continue transborder data transfers with EU Member states. They are to be used solely by U.S. organizations transferring personal information from the European Union to the United States. There are seven safe harbor privacy principles: notice, choice, onward transfer, security, data integrity, access, and enforcement. The principles were developed to qualify U.S. organizations for the safe harbor and the presumption of "adequacy" it creates. Since 1999, U.S. and EU officials have been engaged in informal dialogue concerning implementation of the Directive.

HHS Report and Recommendations

As noted, pursuant to HIPAA, the Secretary of Health and Human Services submitted recommendations to Congress for legislation to protect the confidentiality of health information on September 11, 1997, at a hearing before the Senate Committee on Labor and Human Resources. The recommendations were intended to serve as guidance to Congress in developing legislation, but the report did not contain specific draft language. HHS recommended that a new national law provide a baseline standard for protecting the privacy of health information, and that stronger state laws would continue to apply.

The report outlined five key principles that HHS believed must serve as the foundation for legislation to guarantee privacy of individually identifiable health information:

- Limit, with few exceptions, the use of an individual's health care information to health purposes only;
- Require organizations that are entrusted with health information, including providers and payers, service organizations, organizations receiving information for specified purposes without patient authorization, organizations receiving information pursuant to a patient's authorization, and employers, to provide adequate security measures to protect that information from misuse or disclosure;
- Provide patients with new rights to control how their health information is used, such as the ability to get copies of records and propose corrections;
- Hold those who misuse personal health information accountable, and provide redress for persons harmed by its misuse through criminal and civil penalties; and
- Balance privacy protections with public responsibility to support national priorities, including public health, research, quality care, and reduction of fraud and abuse, including allowing law enforcement access to personal health information within existing law.

While the report was praised for recommending minimum federal standards to provide safeguards for individually identifiable health records and establishing a code of fair

information practices for medical records, it was also criticized for failing to recommend constraints on law enforcement access to health information. At a second Senate Labor and Human Resources Committee hearing on October 28, 1997, various stakeholders commented on the HHS recommendations. They highlighted additional differences of opinion about federal preemption of state laws and access to personally identifiable records for health research. In addition, they emphasized the reliance on federal legal standards for disclosure of health records for treatment and payment, rather than informed consent, as the primary mechanism for protecting patient privacy.

State Laws

On the state level, a patchwork of laws provides certain protections for medical information; however, coverage is considered uneven. The increasing need for providers and insurers to transmit personal medical information across state lines has raised the importance of a comprehensive nationwide legal and regulatory structure. A compendium of state laws issued July 20, 1999 by Georgetown University's Health Privacy Project, *The State of Health Privacy: An Uneven Terrain*, identifies medical records privacy provisions from state legislative codes. The report covers only state statutes and divides them by patient access, restrictions on disclosure, privilege, and condition specific requirements. Offering a more in-depth summary for Florida, Maryland, New York, and Washington, the report is available at [http://www.healthprivacy.org/resources/statereports/contents.html].

The State Public Health Privacy Project has produced a final version of a Model State Public Health Privacy Act. The project sought to develop a model state law addressing information held by public health departments at the state and local levels, with special consideration of HIV/AIDS. It is available at [http://www.critpath.org/msphpa/privacy.htm].

Key Issues

There is general consensus that a federal statute that provides baseline medical records privacy protection would improve safeguards over the existing patchwork of state and federal laws. There also is strong support for a legislative solution to this issue, rather than relying on federal regulations to protect health privacy rights. The bills introduced to date have sought to place restrictions on the use and disclosure of personally identifiable health information, establish security and auditing capabilities for records systems, ensure patient access to their records, provide the right to seek corrections, require entities to provide notices of their privacy practices, and establish penalties for abuse of privacy rights. The bills have varied on the methods for assuring protection, the relationship between federal law and state law, the mechanisms for acquiring informed consent or the use of federal statutes as the basis for allowable disclosures, the rules governing the use of protected health information in conducting research, and procedures for law enforcement access to confidential health information. In addition, the bills have differed in terms of the scope of protected health information covered and the definitions used for such concepts as "non-identifiable health information."

Relationship to Other Laws

The appropriate relationship to state law has been a hotly debated aspect of the discussion about the development of a comprehensive federal law. The question is the desirability of enacting federal medical privacy legislation that preempts, either in whole or in part, state privacy laws. In some areas of law, few states are generally regarded either as having stronger privacy protections for certain types of information or as having acted in an area not covered by federal law. Examples include the areas of mental health, public health reporting, and privileges (such as the physician-patient privilege). While it is recognized that enhanced privacy protections may be desirable for certain types of medical information, the lack of uniformity among the states is often advanced by advocates as the primary reason to seek total federal preemption. Opponents of preemption counter that some of the more stringent provisions of some state laws could be lost with a uniform federal statute. A federal statute need not be totally preemptive, and could preserve some areas for state law application. For example, the HHS recommendations support the concept of federal preemption serving as a floor to which more stringent state laws could be added.

To date seven proposals have been introduced in the 106th Congress that seek to provide a comprehensive scheme for protecting confidentiality.

- The Medical Information Privacy and Security Act, S. 573/H.R. 1057, would preempt state laws that provide less protection than or that conflict with the provisions of the bill. The bill specifically saves from preemption state laws concerning the reporting or disclosure of vital statistics, abuse or neglect, mental health, and a minor's access to health care services and information.

- The Health Information Privacy Act, H.R. 1941, would not preempt state laws that provide either greater protection of health information or greater rights to individuals regarding protection of their health information. An individual may seek an advisory determination from the Secretary of Health and Human Services about whether a particular state law provides for greater protection. Generally, a person relying on an advisory determination will not be subject to penalty or liability. However, a person may not rely on an advisory determination if it conflicts with a decision by a federal or state court that has considered the issue of whether a state law provides greater protection or more rights in regard to health information. Specifically, the act would not preempt any laws regarding reporting of vital statistics; abuse, neglect, or violence against an individual; notification for purposes of emergency response to exposure to infectious diseases; the Americans with Disabilities Act of 1990; and privileges available for health professional peer review activities. The act also would not prevent the use or disclosure of health information by Department of Veterans Affairs to determine eligibility or entitlement to veterans' benefits. Further, the bill states that an individual's disclosure of health information for purposes of obtaining or paying for health care may not be interpreted as waiving a privilege the individual would otherwise have in a state or federal court. The bill also seeks to protect the ability of Congress to obtain information necessary to fulfil its legislative or oversight duties.

- The Health Care Personal Information Nondisclosure (PIN) Act of 1999, S. 578, would not preempt state laws regarding medical information privacy enacted before the act takes effect, as long as such laws provide at least the level of protection provided under the act. Once the act takes effect, 18 months after enactment, it would preempt state laws concerning medical information privacy, except for state law regarding vital statistics, abuse or neglect, public or mental health, minor access to health services and information, and limited use by health care entities.

- The Consumer Health and Research Technology (CHART) Protection Act, H.R. 2455, would preempt state laws that relate to matters covered by the Act. The bill would not preempt any state or federal law regarding the disclosure of a minor's medical information to a parent or guardian. Further, the bill would not preempt any federal law or regulation regarding an individual's access to her own medical information or to health services. State law or regulation concerning medical information about vital statistics, abuse or neglect, public or mental health, or a minor's access to health services and information would not be preempted by the bill.

- The Medical Information Protection and Research Enhancement Act of 1999, H.R. 2470, would preempt state laws that relate to matters covered by the Act. The bill would not preempt any state or federal law regarding the disclosure of a minor's medical information to a parent or guardian. Further, the bill would not preempt any federal law or regulation regarding an individual's access to her own medical information or health services.

- The Medical Information Protection Act of 1999, S. 881, would preempt state laws that provide lesser protections than those in the Act or that conflict with its provisions. However, S. 881 would not apply to a federal or state law regarding disclosure of protected health information about a minor to a parent or guardian. Preemption has also been addressed in patient protection bills where at least one bill, with some exceptions, would preempt most state laws (H.R. 448). The other patient protection bills do not address preemption of similar or stronger state laws (S. 240, S. 6, H.R. 358, S. 300, S. 326, H.R. 216).

Fair Information Practice

The fundamental elements of a code of fair information practice include (1) prohibiting secret personal data recordkeeping systems; (2) providing individuals with a right of access to records being maintained about them and information about how such records are used; (3) providing individuals with a right of action to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent; (4) providing individuals with a right to amend incorrect personal records about them or to supplement such records; and (5) requiring any organization creating, maintaining, using or disseminating records of identifiable personal data to assure the reliability of the data for their intended use and to take reasonable precautions to prevent misuse of the data. There appears to be strong consensus that such principles should be part of any legislation proposed to provide protection of medical records privacy. However, concerns exist about accessing

information about other individuals, accessing information that may be harmful to the patient, and allowing others than the primary creator or holder of the data to make changes to the records. Physicians, in particular, are concerned that non-medical personnel not be authorized to make changes to diagnostic and treatment records.

Principles of fair information practice received expression in most cases in the initial titles of the proposals, under headings concerning "fair health information practices" , "individual's rights", and "rights of protected individuals" in the bills introduced thus far in the 106th Congress (H.R. 1057, H.R. 1941 S. 573, S. 578, and S. 881). They also received some expression in the proposed Patient's Bill of Rights measures in titles concerning the "confidentiality of health information" (H.R. 4250) and "individual rights" (S. 2330). Patient's Bill of Rights legislation and similar proposals offered in the 106th Congress continue to include some fair information practice principals (H.R. 216, H.R. 358, H.R. 448, S. 6, S. 240, S. 300, and S. 326).

Authorization of Access/Informed Consent

While the traditional method of executing control over personal information through informed consent achieves reasonable confidentiality between physician and patient, personal data today are disclosed to multiple secondary users. Informed consent within this integrated system has become impaired and no longer provides adequate protection of privacy (See: Lawrence O. Gostin, *Personal Privacy in the Health Care System: Employer-Sponsored Insurance, Managed Care, and Integrated Delivery Systems,* Kennedy Institute of Ethics Journal, 7.4, 1997, 361-376).

There is agreement, as reflected in all of the medical records privacy bills introduced to date, that use and disclosure must be justified based upon specific criteria, should be limited to only the specific information necessary to accomplish the permissible objective, and should not be used for unrelated purposes. Provisions in the bills provide procedures for revocation of authorizations and many of the bills have called for HHS to develop model authorization forms. The bills generally have allowed for exceptions for such things as emergencies, certain public health purposes, health care oversight, certain judicial and administrative purposes, certain law enforcement purposes, and health research. The conditions under which these exceptions are allowed, however, has varied in different legislative proposals. At issue is how to balance individual privacy rights against other societal goals, such as providing quality care, controlling costs, and protecting public health. Some of the more controversial areas, such as law enforcement and health research, are addressed below.

Different bills use various approaches for authorizing access to protected health information. For example, in the 106th Congress, S. 573 states that patients may deny use or disclosure of personally identifiable health information for a purpose not related to treatment or billing without losing the ability to receive health care. H.R. 1057 has identical provisions. S. 578 calls for a consolidated authorization for disclosure in connection with treatment, payment and health care operations. It allows an individual to revoke a prior authorization if he or she has agreed to assume personal financial responsibility for the treatment services. S. 881 requires procurement of a single authorization for use and disclosure of protected health information for treatment, payment and health care operations. Health care operations consist of services such as the coordination of health care, including health care management of an individual through risk assessment and case management. H.R. 1941 allows a health

care provider, health care payer or any other person who obtains PHI under the Act (referred to as health information custodian) to use or disclose protected information upon obtaining authorization from the individual. A health information custodian may disclose PHI without authorization, to the extent that the Secretary determines appropriate, to provide, or pay for, health care to an individual. However, PHI cannot be disclosed to render employment decisions, or conduct a marketing or insurance underwriting activity. If health care has been provided to an individual who pays for the care himself or herself, a health information custodian may not disclose to a payer without authorization from the individual.

Law Enforcement Access

One of the most controversial areas in the debate over medical records confidentiality is law enforcement access to medical records. The law enforcement community has traditionally voiced concern about the prospect that enhanced patient privacy protections will interfere with its ability to access medical information for a variety of purposes, such as the use of medical reports for identification purposes, to pursue fugitives from justice, or as evidence of illegal activity. Privacy advocates, on the other hand, seek to prevent expansion of law enforcement's access rights.

The law enforcement issue has become more visible due to the need to access personally identifiable medical records for pursuing cases of fraud and abuse in the health care industry. Because estimates place the cost of fraud and abuse at between 5-10% of total health expenditures by public and private insurance programs, Congress has sought in recent years to establish stronger controls and more severe penalties. (See: Kathleen Swendiman and Jennifer O'Sullivan, *Health Care Fraud: A Brief Summary of Law and Federal Anti-Fraud Activities*, CRS Report 97-895.) As pointed out by the National Committee on Vital and Health Statistics in its report, under provisions in HIPAA, the Attorney General is authorized to "issue an administrative subpoena for any health record in a health care fraud investigation, even without federal funding...[although] the same HIPAA provision also restricts the use of health information against the subject of the record unless the investigation arises out of and is directly related to health care fraud."

The 1997 HHS recommendations to Congress brought considerable attention to this issue. They were criticized for allowing law enforcement officials wide authority to access patient records for investigations or prosecutions. Privacy advocates noted that the law enforcement access proposal lacked specific standards, such as probable cause, or mandatory procedures, including a subpoena or written certification of the need for the information. Critics also pointed to the fact that there were less stringent requirements for law enforcement access to medical records than those provided in other areas, such as health research, or for other types of personally identifiable information, such as electronic mail or video rental records. Resolution of this issue is likely to pose a significant challenge for balancing privacy rights and legitimate criminal investigation needs. The Secretary of HHS responded at the September 11, 1997 Senate Labor and Human Resources hearings that the law enforcement recommendation maintains current law, while providing penalties for misuse of personal health information.

In the 106th Congress, S. 573/ H.R. 1067, S. 578, and S. 881 generally would require a subpoena, warrant, court order, or summons before protected health information could be disclosed for law enforcement purposes. S. 578 and S. 881 also permit disclosure pursuant

to a Federal or State law which requires the reporting of specific medical information to law enforcement authorities. S. 573/H.R 1067 and S. 578 require that the protected health information be destroyed or returned to the person from who it was obtained once the matter or need for the information is completed. S. 573/H.R. 1057 prohibit the use or disclosure of such protected health information in an administrative, civil, or criminal action or investigation against the individual, unless it arises out of, or directly relates to, the inquiry for which the information was obtained. H.R. 1941 would allow a health information custodian to disclose PHI to a law enforcement official for a law enforcement inquiry if the official complies with the fourth amendment to the Constitution. This requirement would not apply to disclosure of PHI for purposes of health oversight.

Health Research

Health research has also been one of the most contested areas in the confidentiality debates. A major issue is whether researchers should be required to obtain an individual's informed consent or authorization to access identifiable information about that individual. Health researchers fear that such efforts to restrict access to information in medical records would conflict with the goals of improving patient care and public health. For example, requiring informed consent from an individual before disclosure may adversely affect patient-oriented investigations, including outcomes and observational studies done to assess effects of treatments and trends in diseases. In many cases, patients may be difficult or impossible to contact, which may mean that the data set ends up being too small to be statistically significant. Such a restriction also may present a serious barrier to epidemiology and surveillance studies attempting to identify and control communicable diseases and other public health threats.

Many research projects require the use of identifiable records, sometimes without the explicit consent of the individual. Identifiers are needed to avoid duplication of data and to follow the progress of an individual's health condition or the outcome of treatment over time. However, some contend that such studies can be done with anonymized data. Researchers point to the use of Institutional Review Boards (IRBs) as a key method for ensuring that effective oversight of research projects is performed and privacy standards are enforced.

Currently, IRBs, under the Federal Policy for the Protection of Human Subjects, or Common Rule, have the authority to approve, disapprove, or modify research activities involving human subjects that are conducted, supported, or regulated by federal agencies. The Common Rule (56 Fed. Reg. p. 28002-28032, June 18, 1991) generally requires researchers to obtain an individual's informed consent before conducting research involving that individual. Nevertheless, it is unclear if the IRB system can effectively ensure confidentiality. Largely exempt from the Common Rule requirements is "research, involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects."

An IRB may waive informed consent requirements if it finds that the research involves no more than minimal risk; the waiver will not adversely affect the individual's rights and welfare; the research could not be practicably done without the waiver; and whenever appropriate, the individual will receive additional information after participation.

Another issue is the probability that the current IRB system does not adequately assure confidentiality. According to a 1997 report to the Secretary of HHS, "it is less clear that IRBs have been attending as vigorously to privacy risks as they have to physical and emotional risks." (William W. Lowrance, *Privacy and Health Research*, A Report to the U.S. Secretary of Health and Human Services, Washington, D.C., May 1997, p. viii.). Confidentiality concerns about IRBs were emphasized by GAO in testimony before the Senate Committee on Health, Education, Labor, and Pensions on February 24, 1991. (U.S. General Accounting Office. *Medical Records Privacy: Uses and Oversight of Patient Information in Research*, GAO/T-HEHS-99-70). Privately funded research is not subject to IRB review.

In 1997, HHS recommended to Congress that protected health information be disclosed to researchers without a patient's authorization, but only if the research would be useless to do without identifiers and the project has been approved by an IRB. In the 106th Congress, S. 578 allows an entity to disclose protected health information to a health researcher if the research is federally conducted or supported and complies with the Common Rule; a clinical investigation and conforms with the Food and Drug Administration confidentiality requirements; or, is not subject to the Common Rule. S. 578 requires the Secretary of HHS to submit recommendations on privacy standards of individually identifiable health information in research not subject to the Common Rule to the Senate Labor and Human Resources Committee (now Health, Education, Labor and Pensions Committee) within one year after the act's enactment. In addition, if privacy standards for this research have not been adopted within 2 years after enactment, the Secretary is directed to promulgate final regulations containing such standards within the following 6 months.

S. 881 permits disclosure of protected health information to a health researcher by a person who lawfully possesses it, if an IRB has approved the research project pursuant to requirements of the Common Rule. S. 881 also allows disclosure for analyses of health care records and medical archives if the research: has been reviewed by a board, committee, or other group formally appointed by a person who legally possesses the protected information; and, involves analysis of protected health information previously created or collected by the person. In addition, the person who maintains the protected information to be used in the analyses must: have in place a written security and confidentiality policy; enter into a written agreement with the health researcher that specifies permissible and impermissible uses of the protected information; and, keep a record of all health researchers to whom the protected information has been disclosed. S. 881 also permits disclosure of protected health information to drug, biologic, or medical device manufacturers associated with monitoring activity or reports made to them in verifying safety and efficacy of approved products in special populations or for long-term use.

S. 573 and H.R. 1057 require that all health research, including research that currently falls outside the Common Rule, comply with 45 CFR 46 (Protection of Human Subject) requirements. The bills direct the Secretary of HHS to first promulgate regulations to implement the requirements for all health research to comply with 45 CFR 46. Both bills also require removal of identifiers as soon as possible consistent with the project's purposes, unless an IRB determines a health or research justification for retention and an adequate protection plan has been developed. The patient protection bills contain no specific health research provisions. H.R. 1941 permits disclosure of PHI for health research without obtaining an authorization, but only for uses that have been approved by an entity certified by the Secretary. The Secretary may promulgate regulations that at a minimum: require that

a certified entity first determine that the importance of the health research outweighs intrusion into the privacy of the individual who is the subject of the PHI; and it would be impracticable to conduct the project without using PHI.

LEGISLATION

H.R. 1057 (Markey)
Medical Information Privacy and Security Act. Introduced March 10, 1999; referred to Committees on Commerce and the Judiciary.

H.R. 1941 (Condit)
Health Information Privacy Act. Introduced May 25, 1999; referred to the Committees on Commerce and Government Reform.

H.R. 2404 (Murtha)
Personal Medical Information Protection Act of 1999. Introduced June 30, 1999; referred to Committee on Commerce.

H.R. 2455 (Shays)
Consumer Health and Research Technology (CHART) Protection Act. Introduced July 1, 1999; referred to Committee on Commerce.

H.R. 2470 (Greenwood)
Medical Information Protection and Research Enhancement Act of 1999. Introduced July 2, 1999; referred to Committee on Commerce.

S. 573 (Leahy)
Medical Information Privacy and Security Act. Introduced March 10, 1999; referred to Committee on Health, Education, Labor and Pensions.

S. 578 (Jeffords)
Health Care Personal Information Nondisclosure (PIN) Act of 1999. Introduced March 10, 1999; referred to Committee on Health, Education, Labor, and Pensions. Hearing held April 27, 1999.

S. 881 (Bennett)
Medical Information Protection Act of 1999; referred to Committee on Health, Education, Labor, and Pensions. Hearing held April 27, 1999.

FOR ADDITIONAL READING

William Lowrance. Privacy and Health Research: A Report to the U.S. Secretary of Health and Human Services, Washington, DC, May 1997. 80 p.
[http://aspe.os.dhhs.gov/admnsimp/PHR.htm]

U.S. Department of Health and Human Services. 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. Washington. September 11, 1997. 81 p.

U.S. General Accounting Office. Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited, February 1999, GAO/HEHS-99-55

CRS Reports

CRS Report RS20500, *Medical Records Privacy: Questions and Answers on the Proposed Federal Regulations*, by C. Stephen Redhead.

CRS Report RL30006, *Genetic Information: Legal Issues relating to Discrimination and Privacy*, by Nancy Lee Jones.

CRS Report 98-964, *The Health Insurance Portability and Accountability Act (HIPAA): Summary of the Administrative Simplification Provisions*, by Celinda Franco.