Federal Legislation on Confidentiality: Possibility or Insurmountable Challenge?

Save to myBoK

by Kathleen A. Frawley, JD, MS, RHIA (formerly RRA)

HIM professionals know that keeping health information secure and confidential is one of their most important charges. History concurs. Here's an overview of the confidentiality debate and a look at the future.

For the past 70 years, the American Health Information Management Association and its members have assumed responsibility for protecting the confidentiality of patient health information. This responsibility has never been taken lightly. In recent years, increased access to and use of individually identifiable health information for many purposes have complicated efforts. With the increasing deployment of information technology, consumers are more concerned than ever about the confidentiality and security of health information.

The primary goal of confidentiality is to allow patients to communicate with their physicians and to share information regarding their health status. Trust is an essential element in the relationship between patients and healthcare providers. One of the most important aspects of this relationship is the provider's duty to maintain the confidentiality of health information. The historical origin of a physician's obligation, for example, is found in the Oath of Hippocrates, written between the sixth century BC and the first century AD: "What I may see or hear in the course of treatment in regard to the life of men, which on no account must spread abroad, I will keep to myself..." Ethical codes promulgated by associations of healthcare professionals have consistently recognized the importance of confidentiality. However, these codes do not address current issues regarding use and disclosure of health information.

While communications between patients and physicians are privileged in most states, the protection of these statutes is very narrow. The privilege only applies when a physician is testifying in court or in related proceedings. Many of these statutes include significant restrictions that further limit the availability of the privilege. The physician-patient privilege offers patients no real protection regarding the confidentiality of their health information.

Historical Precedents

In 1928, US Supreme Court Justice Louis Brandeis first identified the basic constitutional principle of privacy:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of a man's spiritual nature, of his feelings and his intellect. They knew that only a part of the pain, pleasure, and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of an individual, whatever the means employed, must be deemed a violation of the 4th Amendment.[1]

In 1973, the US Department of Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens proposed a code of fair information practices based on the following principles:

- openness, which provides that the existence of record-keeping systems and databanks containing data about individuals be publicly known, along with a description of main purpose and uses of the data

- individual participation, which provides that each individual should have a right to see any data about himself or herself and to correct or remove any data that is not timely, accurate, or complete
- collection limitation, which provides that there should be limits to the collection of personal data, that data should be collected by lawful and fair means, and that data should be collected, where appropriate, with the knowledge or consent of the subject
- data quality, which provides that personal data should be relevant to the purposes for which they are to be used and should be accurate, complete, and timely
- use limitation, which provides that there must be limits to the internal uses of personal data and that the data should be used only for the purposes specified at the time of collection
- disclosure limitation, which provides that personal data should not be communicated externally without the consent of the data subject or other legal authority
- security, which provides that personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, or disclosure. Sufficient resources should be available to offer reasonable assurances that security goals will be accomplished
- accountability, which provides that record keepers should be accountable for complying with fair information practices

The Privacy Act of 1974[2] was one of the first applications of this code of fair information practices. The Privacy Act was designed to provide private citizens some control over the information collected about them by the federal government. Healthcare facilities operated by the federal government, such as the Indian Health Service, the Veterans Administration, and the Department of Defense, are bound by the Act's requirements regarding access, use, and disclosure of health information. However, the provisions of this law do not apply to health information maintained in the private sector.

In 1980, the Federal Privacy of Medical Information Act was considered in the 96th Congress. However, the effort to pass federal legislation based on a code of fair information practices was unsuccessful. During the 1980s, the National Conference of Commissioners on Uniform State Laws developed the Uniform Healthcare Information Act in an attempt to stimulate uniformity among states on healthcare information management issues. AHIMA was actively involved at the state level to encourage adoption of this model legislation. However, few states enacted it.

Current Status

Currently, no uniform national standard protects the confidentiality of health information. Rather, health information is protected by state statute or regulation. At the present time, not all 50 states have statutes or regulations that allow patients access to their health information. A review of existing statutes reveals that in some states patients may only access hospital records, while in other states they may access both hospital and physician records.

There is little uniformity among state statutes and regulations regarding confidentiality of health information. Protections vary according to the holder of the information and vary for different types of information. Most statutes do not address redisclosure of health information and lack penalties for misuse or misappropriation. However, many states have enacted specific statutes or regulations regarding sensitive health information (mental health, HIV/AIDS, or genetic information) that impose specific requirements on its handling.

In February 1993, to address the need for federal legislation, AHIMA drafted model legislative language that outlined a code of fair information practices. This language was published in the Office of Technology Assessment report *Protecting Privacy in Computerized Medical Information*[3] as a model code and was used in the drafting of several bills in the 103rd, the 104th, and the 105th Congress.

AHIMA's Position

A number of key provisions in AHIMA's model language are essential elements of any federal legislation to govern the collection, use, and disclosure of healthcare records. These include the following principles of fair health information practices:

- Patient's right to know -- the patient or the patient's representative has the right to know that healthcare information concerning the patient is maintained by any person and to know for what purpose the healthcare information is used
- Restrictions on collection -- healthcare information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected
- Collection and use only for lawful purpose -- healthcare information must be collected and used only for a necessary and lawful purpose
- Notification to patient -- each person maintaining healthcare information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides healthcare information directly to a person maintaining healthcare information should receive a copy of the statement of a person's fair information practices and should receive an explanation of such fair information practices upon request
- Restriction on use for other purposes -- healthcare information may not be used for any purpose beyond the purpose for which it is collected, except as otherwise provided
- Right to access -- the patient or the patient's representative may have access to healthcare information concerning the patient, has the right to have a copy of such healthcare information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such healthcare information of any amendment or correction of such healthcare information requested by the patient or patient representative
- Required safeguards -- any person maintaining, using, or disseminating healthcare information shall implement reasonable safeguards for the security of the healthcare information and its storage, processing, and transmission, whether in electronic or other form
- Additional protections -- methods to ensure the accuracy, reliability, relevance, completeness, and timeliness of the healthcare information should be instituted. If advisable, additional safeguards for highly sensitive healthcare information should be provided

Many individuals have never seen their personal health records and are unaware of the information contained in them. AHIMA strongly believes that individuals have the right to know who maintains their health information and for what purpose the information is used. The improper use or release of this extremely personal and sensitive information may cause significant harm to an individual's ability to obtain employment, education, insurance, credit, and other necessities.

Health information concerning an individual must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected. There must be limitations on the use and disclosure of individually identifiable health information. Regardless of the use or users, individuals must be assured that the information they share with healthcare providers will remain confidential.

AHIMA recommends that the enactment of comprehensive federal preemptive legislation include protections for genetic information. Segregating and creating special protections for specific types of information (i.e., mental health or genetic information) could result in inadvertent breaches of confidentiality by requiring different standards for the handling of this information.

Key Issues

During the 105th Congress, six bills were introduced regarding confidentiality of health information:

1. The Fair Health Information Practices Act of 1997 (HR 52)

2. The Medical Privacy in the Age of New Technologies Act of 1997 (HR 1815)
3. The Consumer Health and Research Technology Protection Act (HR 3900)
4. The Medical Information Privacy and Security Act (S1368)
5. The Healthcare Personal Information Nondisclosure Act (S 1921)
6. The Medical Information Protection Act of 1998 (S 2609)

However, none of these bills were considered for legislative action prior to the end of the 105th Congress.

Since proposed legislation affects patients, providers, insurers, managed care organizations, accreditation organizations, employers, public health officials, health services researchers, and law enforcement personnel, a number of complex issues must be resolved for federal legislation to be enacted.

Some of the key issues are:

- Who should have access to individually identifiable health information?
- How much information should they have access to?
- When can individually identifiable health information be disclosed without patient authorization?
- Should federal legislation preempt state statutes and regulations on confidentiality?
- Should health researchers use individually identifiable health information without patient authorization?
- Should patients have the right to segregate their health information?

During hearings held in the 105th Congress, a variety of perspectives came to light regarding the need for federal preemptive legislation and the scope of that legislation. Some groups advocate that the proposed bills were not strong enough to protect the privacy rights of patients. Other groups are concerned as to how health information is currently used outside the treatment setting, particularly in the areas of law enforcement activities and employment. Other groups that use health information to assess utilization of services and outcomes of care are concerned that legislation will inhibit the flow of information and make information less available for case management, disease management, and other healthcare operations.

One of the most complex questions focuses on the issue of federal preemption. Since the states are responsible for the public health of their citizens, the federal government typically is reluctant to intervene in areas that are considered to be in the domain of the states. Additionally, various groups in the debate advocate different approaches. Three approaches have been advocated:

1. Preempt most state statutes and regulations except those pertaining to mental health and public health
2. Do not preempt state statutes that would provide a greater level of protection for individually identifiable health information
3. Preempt all state statutes and regulations and establish a strong, uniform national standard

A number of groups advocate that federal legislation should not preempt any state statute that provides special protection to mental health, HIV/AIDS, or genetic information. However, AHIMA and a number of our alliance partners believe that all health information deserves the same equally high level of protection and that we should not create "carve-outs" for sensitive information. This is a difficult issue because the real problem is the use of health information to discriminate against an individual. Accordingly, AHIMA has urged Congress to pass strong confidentiality legislation and strengthen anti-discrimination statutes that would prohibit the use of health information for inappropriate purposes.

Prospects for Passage in the 106th Congress

The major impetus for legislation has been the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[4] HIPAA required the Secretary of Health and Human Services, in consultation with the National Committee on Vital and Health Statistics, to submit detailed recommendations on standards with respect to the privacy of individually identifiable health information to Congress in August 1997. The secretary provided her recommendations to Congress at a hearing held by the Senate Labor and Human Resources Committee in September 1997. Congress has until August 1999 to enact legislation on confidentiality of health information. If Congress fails to act by August 1999, the Secretary of Health and Human Services is required to promulgate final regulations containing such standards by February 2000.

Members of Congress and key staff are well aware of the looming deadline. In his most recent State of the Union address, President Clinton stated, "As more of our medical records are stored electronically, the threats to our privacy increase. Because Congress has given me the authority to act if it does not do so by August, one way or another, we can all say to the American people, we will protect the privacy of medical records, and we will do it this year." But because of the complex issues involved, prospects for passage of legislation in the first session remain uncertain. AHIMA has maintained a strong leadership position on this issue and will continue to advocate for the need for comprehensive legislation.

Notes

1. *Olmstead v. United States*, 277 U.S. 438 (1928).
2. Public Law 93-579, 5 U.S.C. §552a
3. Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information.* Washington, DC: US Government Printing Office, 1993.
4. Public Law 104-191.

***Kathleen Frawley** is AHIMA's vice president of legislative and public policy services.*

Article citation:
Frawley, Kathleen A. "Federal Legislation or Confidentiality: Possibility or Insurmountable Challenge?" *Journal of AHIMA* 70, no.3 (1999): 18-22.