National Health Information Privacy Bill Generates Heat at SCAMC

With the introduction of the Bennett bill in the U.S. Senate (S.1360—the Medical Records Confidentiality Act of 1995), a great deal of attention is being focused on the issue of health information privacy. This bill is the result of the work of a bipartisan group of people from public- and private-sector organizations who have been working together over the past two years (and longer for some) to deal with the absence of nationally uniform privacy regulation for health information and the increasing public concerns that arise as more and more health information is being stored and transmitted electronically. Virtually all of the breaches of confidentiality of sensitive health information are now perpetrated by people who have legitimate access to the information, not by unauthorized people who hack into computer systems. Although these breaches cannot be prevented by technology, audit trails and a legal basis for punishment are important first steps in discouraging them. Technical means for securing health information systems are also critical to raise confidence and allay the fear many people experience when they first learn about the power of electronic medical records, and because the current situation may change quickly as more and more people become technically competent with computers and networks. The informatics community, hospital and professional associations, information and communication system vendors, and most of the privacy community are in support of this bill because it enables the cost-effective construction of electronic information systems which will work within the laws of every state while vastly improving the privacy protections for personal health information.

This bill regulates disclosure of “protected” health information, that health information which can reasonably be associated with a specific individual, by making most disclosures dependent on informed consent. It defines as “trustees” people (like providers) and organizations (like employers) who might obtain such information in order to regulate their disclosure of that information. The bill is permissive, in the sense that it allows disclosures to be made by different types of trustees for specific purposes under conditions that are more restrictive than currently used, but does not require disclosure by anyone.

The bill gives patients the rights to inspect, copy, and amend their medical records, with a few specific exceptions where such access could be detrimental. It requires all record holders of protected health information to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the security, integrity, and confidentiality of that information. Information must be identified as protected when it is disclosed and trustees must record all disclosures of that information for purposes other than treatment.

Under this bill, a trustee can disclose protected health information only for a purpose authorized by the bill. In general, permissible disclosures must be compatible with and related to the purpose for which the information was collected or received and are limited to the minimum amount of information necessary. An entity that receives protected health information for one purpose cannot use it against the individual for another purpose. A patient’s consent to disclosure must be informed, time-limited, and more specific than now required. Patients can prohibit otherwise permissible disclosures if they object in writing.

Subject to the general principles stated above, several types of disclosure are permitted (but not required) without specific authorization. Trustees would be able to disclose protected health information for the purpose of protecting the health or safety of an individual from imminent harm; cooperating with an oversight function authorized by law; fulfilling a legally authorized public health reporting function, investigation, or intervention; and performing health research authorized by an institutional review board. Trustees would be able to disclose protected health information subject to a court’s rules of procedure for specified judicial and administrative purposes. Trustees would be able to disclose protected health information to law enforcement authorities to investigate or prosecute a health information trustee, or to respond to a warrant, subpoena, or summons under specified rules of notification and challenge.

Unauthorized disclosures of protected health information would be subject to criminal sanctions, civil lawsuits, and administrative penalties, which would apply to those who knowingly obtain, as well as to those who knowingly disclose the information. Criminal penalties would range from fines of up to $50,000...
and prison terms of up to one year for wrongful disclosure or obtaining of protected health information, to fines of up to $250,000 and prison terms of up to ten years for offenses committed with intent to sell or buy protected health information for commercial advantage, personal gain, or malicious harm.

This bill would preempt State laws except those that prevent or regulate the disclosure of mental health or public health information, vital statistics, or neglect or abuse information.

The topic of this bill led to some very emotional discussions at the recent SCAMC meeting because people believe passionately in diametrically opposed positions, and both ends of the continuum found things to worry about in the bill. A patient rights activist misinterpreted the classification of employers as "trustees" to mean that employers were being given access to protected information, when in fact this classification simply brings employers under the jurisdiction of the law to make them subject to limits on uses and disclosures of information they already have. Likewise, the permission to disclose to law enforcement under specified conditions was interpreted as opening the doors to violations of patient confidentiality, when the bill actually tightens existing requirements for documentation, notification, and opportunities for challenge before such disclosure is even permissible. An informatician read the bill and found that it would prevent physicians from looking at their own medical records before a patient's next visit (because of the time limit on authorizations) and felt that it would stop the legitimate exchange of patient information between institutions because administrators would fear being thrown into jail if a disclosure happened by accident. Before completely understanding the institutional review board provisions, a clinician felt that the bill would prevent the use of health information in clinical research. These interpretations are clearly not the intent of the bill as written, but some of them have legitimate bases that must be addressed in the language. Clearly, some work remains to be done to further clarify the language and educate people about the intent.

As several discussants have stated, a bill such as this is always a compromise between extremes; a tradeoff between absolute individual privacy and practical implementation, costs, and the public good. Once it is fully understood, most people realize that the Bennett bill is much better than the status quo. Finding the fine line between competing extremes that can satisfy most people is the definition of the process of legislation in which we are now engaged. The bill is now (November 95) under active consideration by the Senate Committee on Labor and Human Resources. Watch for the introduction of a similar bill in the House of Representatives and follow that process as well. I encourage you to educate yourself about this important bill. These are the opinions of the author and do not necessarily reflect the opinions of the University of Colorado or the Department of Health and Human Services. For an electronic copy of the Bennett bill or to open a discussion about particular issues, feel free to contact me.

WILLIAM R. BRAITHWAITE, MD, PhD

Correspondence and reprints: William R. Braithwaite, MD, PhD, Associate Professor, Section on Medical Informatics, Department of Preventive Medicine and Biometrics, University of Colorado School of Medicine, Campus Box B-119, 4200 East 9th Avenue, Denver, CO 80262-0119. e-mail: billb@osaspe.ssw.dhhs.gov

Dr. Braithwaite is currently being leased to the U.S. Department of Health and Human Services.

Received for publication: 11/3/95; accepted for publication: 11/3/95.