Affiliation of the author: University of Cincinnati, Cincinnati, Ohio.

Correspondence and reprints: Nancy M. Lorenzi, PhD, University of Cincinnati, Medical Center, P.O. Box 0063, 250 Health Professions Building, Cincinnati, OH 45267-0663; e-mail: ⟨lorenzi@uc.edu⟩.

Received for publication 12/29/99; accepted for publication: 12/29/99.

■ **JAMIA.** 2000;7:204–205.

■

An AMIA Perspective on Proposed Regulation of Privacy of Health Information

As part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress set a deadline for itself of Aug 21, 1999, to pass comprehensive confidentiality legislation. Because Congress failed to meet this deadline, according to the provisions of HIPAA, the Secretary of the Department of Health and Human Services (HHS) is required to issue final regulations by Feb 21, 2000. On Nov 3, 1999, the HHS published a Notice of Proposed Rule Making (NPRM) entitled ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR 160–164) pursuant to the requirements of Section 264 of HIPAA. Usually, the public has 60 days from the issuance of the NPRM to comment on the proposed rules. Because of the complex nature of this issue and the large number of anticipated comments from the public, the Secretary extended the deadline of the comment period an additional 45 days. Consequently, it is unlikely that final regulations will be issued by the original Feb 21 deadline. AMIA developed and submitted a formal response to the NPRM, which is published on the AMIA Web site (www.amia.org). This editorial comment summarizes some of the key points contained in the comments to the NPRM.

AMIA has been a strong advocate for enactment of comprehensive federal legislation to protect the confidentiality of personal health information. We believe that routine use of computer-based patient record (CPR) systems holds great promise for improving the quality of health care delivery in the United States while decreasing its costs, consistent with the Institute of Medicine's 1991 recommendation that the United States adopt the CPR as an essential technology for health care.[1] However, the potential of this information management tool can be realized only if the public is confident that safeguards can be put in place to protect the confidentiality of individually identifiable health information. We commend the Department of Health and Human Services for its timely publication of its proposed standards. Although in most respects the NPRM is consistent with the confidentiality principles endorsed by AMIA, there are specific provisions of the NPRM that AMIA believes need to be revised or, in some cases, deleted. Key points in AMIA's response are summarized below.

Need for Federal Legislation

One of our overriding concerns, which is shared by HHS, is that the HIPAA legislation limits the scope of HHS regulations to ''covered entities'' (health care providers, health plans, and clearinghouses). Although these entities are clearly important in any legislation or regulation dealing with health information privacy, these entities are but a subset of organizations that acquire, store, and share individually identifiable health information. For example, many Internet health sites routinely gather identifiable health information, yet HIPAA and the NPRM do not provide any protection for individual information stored or disclosed by those entities. Only federal legislation can provide comprehensive protection for all uses and disclosures of individually identifiable health information.

In addition, regulatory and enforcement powers of HHS are limited to the defined covered entities. To compensate partly for this limited scope, the NPRM includes a requirement that covered entities establish contracts with their business partners in an attempt to extend the responsibility to protect confidential health information beyond covered entities. Also, by requiring these contracts to name patients as third-party beneficiaries, the proposed regulations may provide legal grounds for private right action in some

states. Although AMIA is sympathetic to the motivation behind the business partner contracts, we find this to be another compelling reason why federal legislation, not regulation, should be passed to provide equal protection for data no matter who has possession of it.

We also believe that federal health information standards must preempt the patchwork of inconsistent state requirements if they are to provide real assurances of privacy to individuals at a time when health care is increasingly an interstate enterprise. We believe that universal and uniform confidentiality protection is necessary to effectively manage health information. It is virtually impossible to monitor and remain knowledgeable about privacy laws and regulations in all 50 states. Furthermore, it would be impractical in computer systems and impossible on paper to reliably apply different state laws to patient data depending on the state in which the patient resides. This situation would force covered entities either to not transmit important clinical data or to attempt to get blanket releases from patients for all routine disclosures. The former situation would be detrimental to patient care, and the latter would defeat the purpose of privacy protection in the first place. Perpetuating the confusion caused by conflicting state regulations could undo the administrative simplification envisioned by the drafters of the HIPAA legislation.

Covered Information

The HHS has interpreted their scope of jurisdiction to cover all health ''information,'' not just information stored on specific media (electronic vs. paper). In the NPRM, however, HHS has elected to cover only information that has been, is, or will be stored or transmitted electronically and exclude coverage of information that has been stored only on paper. AMIA agrees with the Department's interpretation that privacy standards should apply to information, not specific records, but believes that the regulation should cover information in any form in which it is recorded. Consequently, AMIA recommends that the regulations be written to cover all individually identifiable health information, including information stored only on paper. Extending privacy protections to all identifiable health information also eliminates the distinction made in the NPRM between ''individually identifiable health information'' and ''protected health information'' (which excludes information stored only on paper). We believe, simply, that all individually identifiable health information should be protected. From a practical perspective, it would be difficult if not impossible to segregate information that has been, is, or will be transmitted or maintained electronically from purely paper-based information. Because information contained in CPRs can be better protected, we suggest that the Department encourage the use of CPRs as a way of increasing the protection of confidential health information.

Another aspect of covered information is the application of protection uniformly across all data. Although we recognize that some data may be considered more ''sensitive'' than others (based on the potential harm that disclosure may cause), we believe it is more appropriate to raise the overall bar of protection for all confidential health information rather than segregate information by a subjective measure of its sensitivity, which can be different for different people. In addition, we are concerned that special protections that may be afforded certain information on a state-by-state basis would impede the flow of appropriate information among providers caring for individual patients. It is also difficult, in practical terms, to implement different ways to maintain and transmit medical information that comply with various state laws. AMIA believes that all health information should be afforded the same high level of confidentiality protection, regardless of state boundaries.

Right to Restrict Use

AMIA believes that all information in a patient's medical record is important in patient care. Consequently, to allow certain information to be haphazardly included or not included in the medical record could affect the quality of decisions made on the basis of that record. We believe that all information in the medical record should be treated as highly confidential and consequently do not believe that patients should be encouraged or permitted to place additional restrictions on portions of the record. Permitting individuals to request restrictions on the use of subsets of patient data not only compromises the ability of providers to make informed health care decisions, but also creates a potential conflict between the patient's request to restrict access and the provider organization's need to maintain complete medical records.

It would be difficult to predict how a specific patient's request would affect related care decisions. A patient's request to restrict access to information may very well affect future care decisions in ways that were not intended by the patient. For example, a patient might want to limit access to information about his or her diabetes, but not to preventive care reminders. Yet there are aspects of diabetes that would directly affect preventive care reminders of relevance to diabetics. In addition, it would be impossible to guarantee that re-

strictions agreed to by one provider or covered entity would follow the information to the next provider.

De-identification of Information

In an effort to encourage organizations to ''de-identify'' patient information when conducting aggregate data analysis, HHS provided a list of 19 data elements that should be removed from patient information to render it anonymous. The 19th data element is actually a catchall placeholder for any other distinguishing feature that, when combined with other information, could render information identifiable. Although we applaud the Department's attempt to provide clarity on this subject, defining data as de-identified when these 19 data elements are removed may inadvertently create a false sense of security. With the ever-increasing availability of public databases and the increasing power of computers' computational capability, removal of only the 19 data elements mentioned in the provisions may eventually be inadequate to properly de-identify the information. For this reason, we believe that the use of relative terms such as ''high re-identification potential'' and ''low re-identification potential'' be used to indicate the nonstatic nature of the potential for re-identification of a data set. One of the strengths of the NPRMs for privacy and security is the educational content provided in the provisions. We believe that using these phrases would contribute to that educational process.

Use of Information in Research

AMIA strongly supports the Department's view that all research, both publicly funded and privately sponsored, should conform to common privacy practices. We believe that privacy is a universal right that transcends the funding of a particular research project. The counterpart to Institutional Review Boards (IRBs) overseeing publicly funded research is the privacy board defined in the NPRM for privately funded research. The proposed regulations expand the criteria used to grant a waiver of authorization to use or disclose individually identifiable health information for the purposes of research. The question arises whether current IRBs are appropriately constituted to adequately judge the fulfillment of the four additional criteria. We suggest that the Department complete its planned review of the Common Rule and receive the findings of the Institute of Medicine study recently announced by the Agency for Healthcare Research and Quality in collaboration with the Office of Planning and Evaluation before implementing a change in the role and function of the IRB. In the meantime, the Department could proceed with its requirement that a ''privacy board'' be established to judge whether research projects meet the criteria for disclosure without authorization. An individual organization may choose to use an existing IRB to make this determination.

Minimum Necessary Disclosure

The NPRM stipulates that covered entities are required to utilize the ''minimum amount'' of identifiable health information for all uses and disclosures. AMIA agrees with the concept in principle, as it addresses a major area of concern—the internal use of confidential health information for purposes other than those under which it was originally collected. The Department may want to comment on effective use of CPRs to implement this provision. Many CPRs have provisions to limit access to patient data, which are based on user security permissions, professional roles, and the existence of a professional relationship. In addition, CPRs can filter information so that only those data needed for the purpose of a particular disclosure are transmitted. Ultimately, the only efficient way that an organization can comply with both the security provisions and the privacy provisions of HIPAA is by using a CPR.

In summary, the provisions laid out in the NPRM take the country a major step forward in protecting the confidentiality of individually identifiable health information, but we have much further to go because of the limited scope granted HHS under HIPAA. Congress must not abdicate its responsibility to provide equal protection under the law for all confidential health information. Likewise, AMIA members must take a leadership role in educating and advising policy makers about ways to ensure that the data collected, stored, and manipulated in the systems that we develop and operate are fully protected.—PAUL C. TANG, MD

Reference ■

1. Institute of Medicine Committee on Improving the Patient Record. The Computer-based Patient Record: An Essential Technology for Health Care. 2 ed, rev ed. Washington, DC: National Academy Press, 1997.

Affiliation of the author: Palo Alto Medical Foundation, Palo Alto, California, and Epic Systems Corporation, Madison, Wisconsin.

Correspondence and reprints: Paul C. Tang, MD, Palo Alto Medical Clinic, 370 Distel Circle, Los Altos, CA 94022; e-mail: ⟨tang@smi.stanford.edu⟩.