TexasMedical Association

PHYSICIANS CARING FOR TEXANS

February 17, 2000

Secretary Donna Shalala
U.S. Department of Health and Human Services, Assistant Secretary for Planning and Evaluation
Attention: Privacy-P, Room G-322A
Hubert Humphrey Building
200 Independence Avenue SW
Washington, DC 20201

Re: Standards of Privacy of Individually Identifiable Health Information; Proposed Rule

Dear Secretary Shalala:

The Texas Medical Association is pleased to offer its comments to the Department of Health and Human Service's proposed rule setting standards for privacy of individually identifiable health information published in the November 3, 1999, Federal Register (FR 64, 59919).

Texas Medical Association represents 37,000 physicians in the state of Texas. Our members strongly support patient confidentiality and believe that patients should have the right to keep their medical records private and to refuse disclosure of confidential information for any reason except for treatment and payment purposes. We support the comments offered by the American Medical Association on the broad range of issues affecting all physicians by these proposed regulations and specifically agree that the rights of patients to control the use and dissemination of their health information is essential to safeguard the physician-patient relationship.

Texas Medical Association's comments may be summarized as follows:

1. **Definition of Covered Entities [Section 160.103]**

The proposed regulations provide the following definition of "covered entities": "...health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction referred to in section 1173(a)(1) of the Act. "

TMA is concerned that the proposed rules do not directly apply to many other entities that collect, maintain and disseminate health information such as employers, workers compensation carriers, life insurers, schools, and others. HHS acknowledges this fact in the summary section of the proposed rules. TMA has specific concerns that certain entities may fall outside the scope of the regulations and disclosures for payments may routinely result in disclosures of protected health information to non-covered entities, such as employers. The proposed rule acknowledges that ". .in some cases, a payment activity could result in the disclosure of protected health information by a plan to an employer or to another payer of health care, or to an insurer who is not a covered entity. ."

TMA supports prohibiting disclosure of individually identifiable health information to employers and other non-covered entities. TMA believes that entities, that through the normal course of

their daily activities might have access to protected health information, should be subject to the compliance provisions. Without additional protections, TMA is concerned that there will be instances of unauthorized disclosure of private information to entities not covered under the proposed rules, i.e., employers, schools, workers compensation carriers, and pharmacy benefit management companies.

2. Uses and Disclosures of Protected Health Information without Individual Authorization [Sec. 164.510]

Although the regulations provide that "covered entities" are prohibited from disclosing individually identifiable health information, there are numerous exceptions that permit disclosure in almost every circumstance. Covered entities would be required to develop and document policies and procedures for how protected health information would be used and disclosed by the entity and its business partners. In addition, the regulations require that covered entities include policies and procedures necessary to address disclosures required by applicable law whether or not patient consent is required. TMA opposes the release of individually identifiable health information without a patient's consent.

3. Use and Disclosures for Public Health Activities [Sec. 164.510(b)]

The proposed rules allow covered entities to disclose protected health information for inclusion in State or other governmental health data systems without individual authorization when such disclosures are authorized by State or other law in support of policy, planning, regulatory or management functions. Although TMA supports these government data activities, we oppose any regulation allowing disclosure of individually identifiable health information without a patient's consent for government data collection.

4. Covered Entities and Administrative Requirements [Sec. 164.5181

Covered entities would be required to have in place administrative systems, appropriate to that nature and scope of their business, that enable them to protect health information in accordance with this rule. The proposed rule imposes several burdensome administrative requirements on "covered entities." Specifically, covered entities will be required to: (1) designate a privacy official; (2) provide privacy training to members of its workforce; (3) implement safeguards to protect health information from intentional or accidental misuse; (4) provide a means for individuals to lodge complaints about the entity's information practices, and maintain a record of those complaints; and (5) develop a system of sanctions for members of the workforce and business partners who violate the entity's policies. All covered entities will be required to implement these mandates, from the smallest provider to the largest health plan. Although, the proposed regulations leave the details of implementing these policies to each covered entity, TMA believes that these requirements are overly burdensome on small entities, especially solo practitioners and small group practices.

5. Application to Business Partners [Sec. 164.506(e)]

The proposed rule applies only to certain covered entities: health care providers, health plans, and healthcare clearinghouses. The rule does not, however, apply to "business partners." Under the proposed rule, a "business partner" is defined as:

> ". .a person to whom a covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. Such term includes any agent, contractor or other person who receives protected health information from the covered entity. .for the purposes described in the previous sentence."

These other business partners would include third party billing agents, third party administrators, lawyers, consultants, and auditors. The proposed rule allows entities to disclose protected health information to persons they hire to perform functions on their behalf where such information is needed for that function.

Because covered entities fall under the scope of the proposed rule, but business partners of covered entities do not, the proposed rules require the relevant contract between a covered entity and a business partner contain a provision whereby the business partner is required to ensure that protected information will not be subject to unauthorized release:

We would support covered entities disclosing protected health information to business partners only pursuant to a written contract that would, among other specified provisions, limit the business partner's uses and disclosures of protected health information to those permitted by the contract, and would impose certain security, inspection and reporting requirements on the business partner.

The rule, unfortunately, does not stop there. It states further that "We would hold the covered entity responsible for certain violations of this proposed rule made by their business partners ." Thus, because business partners are not under the authority of the proposed rule, the DHHS attempts to structure their conduct by making covered entities subject to sanctions for the unauthorized release of protected information.

Holding covered entities responsible for the unauthorized release of protected identifiable health information by their business partners is probably beyond DHHS's authority under this rule. Since the rule does not apply to the business partners of covered entities, these business partners cannot violate the proposed rule by improper release of protected information as defined by the rule. When a business partner of the covered entity releases protected information, there can be no violations of the rule. If business partners cannot violate the proposed rule, then DHHS has no authority to sanction covered entities based on the conduct of their business partners.

Since DHHS has no authority over business partners, the only party in a position, under the proposed rule, to sanction the business partner for unauthorized release would be the covered entity via a breach of contract action. But the proposed rule does not require covered entities to enforce their contract provisions through legal action. If DHHS cannot enforce the rule against a business partner, and if the rule does not require enforcement from the private sector, the contract requirement to safeguard protected information will, as a practical matter, be unenforceable.

Holding the covered entity responsible for certain "violations" of their business partners ought to be abandoned because it will impose an undue burden on covered entities. Covered entities are placed in the highly unusual situation in which they have a responsibility to ensure, not only that they do not breach their own contracts, but that the parties with whom they contract, i.e., business partners, do not breach theirs. The rule is unclear as to what is the nature and extent of the

covered entity's responsibility. Does the rule imply that a covered entity must have a monitoring process in place to ensure that a business partner does not perpetuate an unauthorized release of protected information? Making a covered entity responsible for the conduct of its business partners, who are not even regulated under the rule, will impose added financial impediments on organizations who are already burdened by ensuring the compliance of their own personnel. At a minimum, the rule must define the nature and extent of the covered entity's responsibility for the acts of its business partners. The rule should also be amended to require that any business partner must acknowledge that the rule applies to it and that any information obtained by the business partner pursuant to or under this rule retain its status as a medical record.

6. Relationship to State Laws [Sec. 160, Subpart B]

The proposed rules allow for three specific state law preemption: (1) more stringent state protections; (2) regulations that the Secretary determines are necessary to prevent fraud and abuse; and (3) regulations that the Secretary determines are necessary to ensure appropriate state regulations of insurance and health plans and for State reporting on health delivery, and for State laws that address controlled substances.

Pursuant to Section 1178 of HIPAA the proposed rules create a federal "floor," rather than a "ceiling", so that more stringent state protections would stay in force. Section 1178 of HIPAA 178(a)(1) sets out a "general rule" that State law provisions that are contrary to the provisions or requirements of Part C of Title Xl or the standards or implementation specifications adopted or established thereunder are preempted by the federal requirements .three exceptions to this rule follow. ."for State laws relating to the privacy of individually identifiable health information which as provided for by the related provision of section 264(c)(2) are contrary to and more stringent than the federal requirements. Section 264(c)(2) of HIPPA provides that the HIPAA privacy regulations which is proposed subpart B of proposed part 160, will not supersede "a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards or implementation specifications imposed under the regulation at proposed subpart E of proposed part 164."

Generally speaking, the proposed rule would not conflict with the provisions of Texas law. For example, the Texas Medical Practice Act permits the disclosure of medical records to "qualified personnel for research for a management audit, financial audit, or program evaluation so long as the personnel may not directly or indirectly identify a patient in any report for the research, audit, or evaluation or otherwise disclose the identity of the patient in any manner. Further, the Medical Practice Act permits a physician to disclose, without a patient consent, whose parts of the medical records that reflect changes and specific services that the physician has provided if the disclosure is necessary in the collection of fees for medical services provided by the physician, professional association, or other entity qualified to provide or arrange for medical services.

However, some current confidentiality statutes are stricter than the proposed rule and the Medical Practice Act. For example, under the Communicable Disease Prevention and Control Act, no person is permitted to release a test result for HIV to a third party payer or a person conducting a management audit without written consent by the patient. So, for example, a physician could not submit medical records containing HIV information to a third party payer in an effort to obtain reimbursement unless that physician had obtained patient consent to do so.

Obviously, there may be situations in which state law is stricter than the proposed rule, but other instances in which the federal law is stricter than the law of the state. The Association is seeking guidance as to whether a statute like the Communicable Disease Prevention and Control Act would not be preempted because it is stricter than the proposed rule. In either case, the TMA asks that the rule explicitly state that the stricter rule applies, whether it be state or federal, and regardless of whether there is any conflict between state and federal law.

Again, the TMA is pleased to offer its comments to the Secretary's proposed rule for standards for privacy of individually identifiable health information. Should you have any questions about our comments, you may contact Mr. Rocky Wilcox, Office of the General Council, at 512-370-1340.

Sincerely,

Paul B. Handel, MD
Chair. Council on Socioeconomics