Indiana Lawyer October 9, 2002

BASIC HIPAA FOR TRIAL LAWYERS

Karen R. Orr
Trenten D. Klingerman

You may have noticed the numerous seminars, articles, and general tidal wave of information related to HIPAA lately, but thought you could safely route this information straight to the circular file. After all, you are a litigator, not a health care compliance lawyer. Or, maybe you were slightly amused by catchy titles like "Hip Deep in HIPAA" while wondering whether it's HIPPA or HIPAA, and what does it stand for anyway? HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996, and although it has been with us since 1996, new regulations promulgated by Health and Human Services ("HHS") are the subject of the current flurry of seminars, articles, and major headaches. These regulations will undoubtedly have a major impact on health care providers, health plans, and the health care-insurance industry in general, but the effects will reach much further: to anyone needing access to, or use of, personal medical information and records. The privacy regulations promulgated by HHS will become effective on April 14, 2003, and may have some trial lawyers suddenly wondering why the standard subpoenas they have always issued are suddenly insufficient to obtain a plaintiff's medical records.

HIPAA became law on August 21, 1996, as part of the Social Security Administration Act. Part of the legislation, known as the "Administrative Simplification Act," was intended to standardize and improve the efficiency of electronic transactions in health care and to ensure the security and privacy of "individually identifiable health information." On December 28, 2000, HHS issued a final rule establishing "Standards for Privacy of Individually Identifiable Health Information." HHS affectionately calls this the "Privacy Rule." In March 2002, HHS released proposed revisions to the regulations and issued a final rule modifying the Privacy Rule on August 14, 2002. The Privacy Rule is set forth at 45 C.F.R. Parts 160 and 164.

The Privacy Rule is not readily reducible to a short discussion of the requirements, so the following overview and discussion contain many generalizations. The Rule itself has very specific definitions, cross-references, and nuances that should be carefully evaluated.

As the name suggests, the Privacy Rule takes hard aim at protecting the privacy of an individual's health information. For "covered entities," including health care providers who conduct certain electronic transactions, health care clearinghouses, and most health plans, the Privacy Rule requires preparation of a "Notice of Privacy Practices" and implementation of policies and procedures to protect the privacy of a person's medical records and information, and limit requests and disclosures of private medical information. Most health care providers will be covered by HIPAA because most perform at least one of the electronic transactions identified in the Rule (*i.e.* ,electronic payment of claims).

The Privacy Rule broadly defines what health information is "protected" health information ("PHI") and narrowly limits the uses and disclosures of PHI. Generally, an authorization (with specific requirements reviewed below) signed by the individual is required to obtain the information unless the disclosure relates to "treatment, payment, or health care operations" ("TPO"). There are also specific exceptions to the authorization requirement

including, *inter alia*, disclosures that are "required by law." These restrictions will make obtaining medical information a tricky business.

Moreover, the Privacy Rule requires non-covered entities who receive PHI to enter into "business associate" agreements, which require the non-covered recipient to agree to comply with many of the HIPAA requirements imposed on covered entities. Lawyers may be considered "business associates" if they represent a covered health care provider and obtain PHI. Therefore, an attorney hired to defend a covered health care provider in a medical malpractice claim will need a business associate agreement in place with her client before she can obtain PHI.

Although the final Privacy Rule does not expressly contain a private right of action, it is widely believed that noncompliance will generate plenty of lawsuits and that plaintiff's lawyers will be ready to test the waters as soon as compliance is required. Therefore, trial lawyers will need to be familiar with HIPAA by April 14, 2003. The following contains brief overviews for trial lawyers of a few of the major affected areas.

SUBPOENAS

As a general rule, HIPAA privacy regulations preempt all contrary state laws, except in cases where the state law is more stringent than the HIPAA privacy requirement and in a few, specific carve-out exceptions. 45 C.F.R. § 160.203.

A covered entity may not use or disclose PHI without providing the individual an opportunity to provide written consent, authorization, or to object in certain circumstances. 45 C.F.R. § 164.512. The Privacy Rule specifically sets forth the circumstances under which a covered entity may disclose PHI in the course of an administrative or judicial proceeding. 45 C.F.R. § 164.512(e). First, a covered entity may disclose PHI subject to the written authorization of the individual. 45 C.F.R. § 164.502(a)(1)(iv); *see also* 45 C.F.R. § 164.508 (setting forth requirements of an authorization). Second, it may disclose specific PHI in response to a court (or administrative tribunal) order. 45 C.F.R. § 164.512(e)(1)(i). Finally, it may disclose PHI in response to a "subpoena, discovery request or other lawful process" but only if it receives "satisfactory assurance" that the party seeking PHI has made reasonable efforts to either (1) provide written notice of the request to the individual; or (2) obtain a "qualified protective order." 45 C.F.R. § 164.512(e)(1)(ii)(A)&(B). A "qualified protective order" is an order that prohibits the use of PHI for any purpose other than the proceeding in which the order is issued and provides for the return or destruction of all copies of PHI at the conclusion of the proceeding. 45 C.F.R. §164.512(e)(1)(v)(A)&(B).

A covered entity receives "satisfactory assurance" of notice if the requesting party provides the entity with a written declaration and supporting documentation that (1) the requesting party has made a good faith effort to provide the individual with written notice sufficient to permit the individual to raise objections to the disclosure, and (2) the individual has either failed to timely raise an objection to the request or the court (or administrative tribunal) has resolved any objection in the requesting party's favor. 45 C.F.R. § 164.512(e)(1)(iii)(A)-(C). A covered entity has "satisfactory assurance" of the requesting party's efforts to obtain a "qualified protective order" if the requesting party provides the entity with a written declaration and supporting documentation that the requesting party has submitted the proposed order to a court. 45 C.F.R. § 164.512(e)(iv)(A)&(B).

AUTHORIZATIONS

An individual can still authorize the disclosure of his or her PHI under the Privacy Rule. The authorization must contain certain "core elements," including: (1) the name of the individual; (2) a meaningful and specific description of the information to be disclosed; (3) the name of the person or entity who is to receive the information; (4) a description of the purpose of the disclosure; (5) an expiration date or expiration event; and (5) the date and signature of the individual. 45 C.F.R. § 164.508(c)(1)(i-vi). In addition to the "core elements," the authorization must contain the statements concerning: (1) the individual's right to revoke the authorization in writing, the exceptions to the right to revoke the authorization and a description of how the individual may revoke the authorization; (2) the ability (or inability) of the covered entity to condition treatment, payment, enrollment or eligibility for benefits on the authorization; and (3) the potential for the information to be redisclosed by the recipient and to lose its protection from use and disclosure. 45 C.F.R. § 164.508(c)(2)(i-iii). Finally, all authorizations must be written in "plain language." 45 C.F.R. § 164.508(c)(3).

BUSINESS ASSOCIATE AGREEMENTS

Lawyers who are hired to represent covered entities and who need to receive PHI (*e.g.* PHI of a plaintiff or other patients of the client) will be required to execute a business associate agreement with the client. This requirement may seem antithetical to a lawyer's role as advocate and may even seem offensive to some lawyers. Consider the scenario in which the lawyer needs to advise her client about the need for the business associate agreement and then present the client with a draft agreement. Should the lawyer advise her clients to hire another attorney to review it before signing? Perhaps the best reading of the business associate agreement requirement is that the agreements merely formalize what attorneys already have an ethical responsibility to do--keep information received from clients confidential. Moreover, the burdens are imposed in the direction of the business associate lawyer, not the client.

The Privacy Rule states that the covered entity may provide PHI to a business associate if the covered entity receives "satisfactory assurances that the business associate will appropriately safeguard the information." 45 C.F.R. § 164.502(e)(1). These satisfactory assurances must be contained in the form of a written agreement meeting the requirements of 45 C.F.R. § 164.504(e). The requirements are specifically enumerated in the Privacy Rule, and include, *inter alia*, assurances that the business associate will: (1) not use or disclose the PHI except as permitted by the agreement or as required by law; (2) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract; (3) report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware; (4) ensure that any agents to whom it provides information will agree to the same restrictions and conditions imposed on the business associate; (5) make certain information available to the covered entity to meet the covered entity's requirements; (6) make information available to HHS for purposes of determining the covered entity's compliance with the business associate requirements under the Rule. 45 C.F.R. § 164.504(e)(2). The Privacy Rule contains "sample provisions" as an Appendix to the Preamble of the Rule to assist entities and business associates in complying with these requirements.

The foregoing only begins to touch on the many, detailed HIPAA Privacy requirements. For example, the HIPAA Privacy Rule provides individuals with certain protections and rights, including the right to receive a covered entity's "Notice of Privacy Practices," the right to have access to their PHI, the right to request amendments to their PHI, and the right to receive an accounting of disclosures of their PHI for any purposes other than treatment, payment and health care operations, to name but a few. Without question, some lawyers will view HIPAA as a means of creating or revitalizing common law privacy actions. Given the specter of lawsuits and penalties, health care providers will be more reluctant than ever to release protected health information without strict compliance with the Privacy Rule's requirements.

Ms. Orr is a partner and Mr. Klingerman, an associate, with the Lafayette firm of Stuart & Branigin. Ms. Orr is a member of the DTCI Medical Malpractice section.