Analysis&Perspective

Think Health Care Providers Don't Need Patient Consent to Disclose Health Information? Think Again. *A review of the history of consent under the HIPAA privacy rule and an analysis of HIPAA preemption.*

BY GINA M. CAVALIER AND AMY B. KIESEL

Call it what you will —''consent,'' ''authorization,'' or ''release'' — health care providers still may need to obtain some type of legal permission from patients prior to disclosing their health information for certain routine purposes, particularly for disclosures involving sensitive information (*e.g.*, genetics, substance abuse), even though it is no longer required under the federal privacy regulations (''Privacy Rule'') issued under the Health Insurance Portability and Accountability Act of 1996 (''HIPAA'').

HIPAA's preemption standard dictates this result because it preserves most state laws that are more protective of an individual's privacy, such as those that require legal permission where none is required under the Privacy Rule.

On August 14, 2002, the United States Department of Health and Human Services (''HHS'') issued the greatly anticipated final modifications to the Privacy Rule. As noted, as a result of these modifications, health care providers are no longer required to obtain legal permission (specifically, ''consent'') from their patients prior to using or disclosing protected health information (''PHI'') for ''most routine health care delivery purposes'' —referred to as treatment, payment or health care operations (''TPO''). This change represents a significant shift in policy because, in the past, HHS has argued that obtaining patient consent for TPO was crucial to protecting individual privacy rights.

Despite this change in policy at the federal level, legal permission may nevertheless be required under state law, and HIPAA will not preempt such state law requirements. Thus, as a practical matter, health care providers will need to survey applicable state laws to determine the circumstances under which legal permission is required, as well as the specific requirements for the form of such permission.

As discussed below, states regulate health information obtained by health care providers from multiple angles. In particular, state law may require certain types of health care providers (*e.g.*, hospitals, physicians, clinical social workers) to obtain legal permission to disclose health information, even for some TPO. Additionally, many state laws have heightened protection for certain types of ''sensitive'' health information (*e.g.*, information related to genetics, mental health, and human immunodeficiency virus and other communicable diseases) and may require legal permission for many, if not most, disclosures, including those for routine purposes.

Cavalier is an associate in Shaw Pittman's health law group in Washington, D.C. She can be reached at (202) 663-8629, or at Gina.Cavalier@shawpittman.com

Kiesel is a health law associate with the Washington, D.C., office of Hogan & Hartson, and can be reached at (202) 637-5834 or at abkiesel@hhlaw.com

I. Overview of HIPAA Administrative Simplification and the Privacy Rule

Under HIPAA, HHS is required to promulgate a series of regulations designed to increase the efficiency of electronic transactions in the health care industry as well as protect the privacy and security of health information. These provisions are known as the ''Administrative Simplification'' provisions. It is under these provisions that HHS promulgated the Privacy Rule.

The Privacy Rule applies to ''covered entities,'' which include (1) health care providers that submit standard electronic transactions, (2) health plans, and (3) health care clearinghouses. The Rule safeguards PHI maintained by such covered entities. PHI is broadly defined to include most health information that identifies, or could be used to identify, the individual.

Typically, the Privacy Rule is conceptualized into three parts: (1) limitations on ''uses'' and ''disclosures'' of PHI, (2) individual rights, and (3) administrative requirements. Each part is described briefly below.

Covered entities are required to use and disclose PHI *only* as set forth in the Privacy Rule. The Privacy Rule groups disclosures into four categories:

- uses and disclosures for TPO,
- enumerated permissive disclosures,
- disclosures pursuant to verbal agreement (or failure to object), and
- uses and disclosures pursuant to written authorization.

Each category is subject to specific restrictions and limitations, which may include legal permission.

The first category includes disclosures for TPO (*i.e.*, treatment, payment, or health care operations). Covered entities have an *option* to obtain ''consent'' (historically, a short simple form, signed by the individual to use or disclose PHI for TPO); otherwise, they are free to disclose PHI without any legal permission for *their own TPO*. Additionally, the Privacy Rule permits disclosure for treatment and payment activities of *another health care provider or covered entity* and some health care operations of *another covered entity*.

  HLR ISSN 1064-2137

The Privacy Rule defines treatment broadly as including those activities related to ''the provision, coordination, or management of health care and related services by one or more health care providers.'' 45 C.F.R. § 164.501. Payment is defined, with respect to a health care provider, as the activities undertaken ''to obtain or provide reimbursement for the provision of health care,'' which includes eligibility or coverage determinations, billing and claims management, medical necessity reviews, utilization reviews, and disclosures to consumer reporting agencies. *Id*. Health care operations include:

(1) quality assessment and improvement activities;

(2) review of competence and qualifications of health care professionals (*e.g.*, accreditation, licensing);

(3) underwriting, premium rating and other similar activities;

(4) conducting or arranging for medical review, legal services, and auditing functions;

(5) business planning and development; and

(6) business management and general administrative activities.

The second category of disclosures is a list of eleven narrowly defined disclosures that may be made without any type of legal permission. That said, the Privacy Rule sets forth some limitations on most of these disclosures. For example, disclosures are permitted in the context of research; however, a number of other criteria must be met, such as a waiver of an authorization requirement from an institutional review board or privacy board.

The third category of disclosures includes those permitted under certain circumstances where the individual does not object. Specifically, disclosures for notification purposes, for facility directories, or to individuals involved in the patient's care or payment for care are permitted where the patient orally agrees (or does not object) to such disclosure.

Finally, any other disclosure that does not fall within the three categories described above forms the fourth category by default. These disclosures may be made only with the patient's written ''authorization.'' In general, an authorization is a fairly detailed form of legal permission, which specifically describes the circumstances of the disclosure and contains an expiration date or event. Note that authorization may be required for disclosures for certain health care operations of another covered entity (*e.g.*, disclosing PHI to assist another covered entity in conducting medical reviews).

Returning to the three-part structure of the Privacy Rule, covered entities also are required to grant patients certain rights. For example, patients must be given access to certain PHI, must be permitted to amend certain PHI, and must receive an ''accounting'' of certain disclosures of PHI.

Finally, covered entities are required to implement certain administrative policies and procedures. For example, covered entities are required to train members of their work force and establish and implement policies and procedures regarding the Privacy Rule's requirements.

II. History of Consent Under the Privacy Rule for Health Care Providers

A. Proposed Privacy Rule

On Nov. 3, 1999, HHS issued the proposed Privacy Rule. 64 Fed. Reg. 59,918. Importantly, the proposed Privacy Rule did not require health care providers to obtain legal permission in the form of a ''consent'' prior to using or disclosing PHI for the provider's own TPO or that of another individual or entity, with certain limited exceptions (*e.g.*, psychotherapy notes). 45 C.F.R. § 164.506(a)(1)(i) (proposed). In fact, providers were *prohibited* from seeking consent for these purposes, unless required by state or other law, as HHS contended that a consent provided individuals with ''little actual control over information.'' *Id.* § 164.508(a)(2)(iv); 64 Fed. Reg. at 59,940. Further, HHS noted that while many health care providers, in fact, do obtain consent prior to disclosing health information, a patient cannot make a truly informed, voluntary decision when asked to sign a consent at his or her provider's office, as this atmosphere simply is not conducive to accomplishing such goals. *Id*. Finally, HHS stated that its decision to prohibit patient consent was ''intended to make the exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care. For individuals, health care treatment and payment are the core functions of the health care system. This is what they expect their health information will be used for when they seek medical care and present their proof of insurance to the provider.'' *Id.*

B. Final Privacy Rule

A little more than a year later, HHS reversed its position. On Dec. 28, 2000, HHS issued the final Privacy Rule, which *required* a health care provider with a ''direct treatment relationship'' (*e.g.*, most hospitals and physicians) to obtain consent of the patient for the use or disclosure of PHI for TPO. 65 Fed. Reg. 82,462; 45 C.F.R. § 164.506(a) (*prior to revision*). Further, HHS required an even more stringent form of legal permission, authorization, for disclosures that were not for the payment or health care operations of the disclosing covered entity. 45 C.F.R. § 164.508 (*prior to revision)*. Stated otherwise, HHS required a provider to obtain consent for its own TPO and an authorization to disclose PHI for the payment or health care operations of another (disclosure for treatment of another only required consent). As HHS explained, this significant change in policy was a response to comments that it received explaining that consent, in fact, is important because it focuses the patient's attention on the substance of the transaction and provides an opportunity for the patient to understand and seek modifications to the provider's privacy practices. 65 Fed. Reg. at 82,473. Additionally, many health care practitioners felt that the prohibition against obtaining consent interfered with their ethical requirements to do so, and it conflicted with their current practice. *Id.* at 82,648.

C. Modifications to the Final Privacy Rule

Fifteen months later, on March 27, 2002, HHS again changed its position and proposed modifications to the Privacy Rule. This time, it did not set forth any absolutes—instead, health care providers were permitted, but not required, to obtain consent to disclose PHI for their own TPO. 67 Fed. Reg. 14,776; 45 C.F.R. § 164.506. Further, the proposed modifications permitted disclosures (irrespective of whether consent was obtained) for treatment and payment activities of *another covered entity or health care provider* and for certain health care operations of *another covered entity*. 45

C.F.R. § 164.506(c)(2) – (4). Specifically, disclosures for health care operations of another covered entity are permitted without consent only if both entities (*e.g.*, holder and recipient) have a relationship with the patient and the disclosure is: (1) for quality assessment and improvement activities, for reviewing the competence or qualifications of professionals, for training, and for licensing/accreditation, or (2) for the purpose of health care fraud and abuse detection or compliance. All other disclosures for the health care operations of another covered entity require authorization.

In lieu of consent, the Privacy Rule requires providers with a direct treatment relationship to make a good faith effort to obtain an individual's written acknowledgment of receipt of notice of privacy practices. *Id.* § 164.520(c)(2)(ii). HHS attributed this change in policy to concerns raised by health care providers that the ''consent requirements will impede access to, and the delivery of, quality health care.'' 67 Fed. Reg. at 14,779. Interestingly, HHS stated in contrast to comments on the Final Privacy Rule that many providers currently do not obtain consent for disclosing PHI for TPO. *Id.* at 14,780.

On Aug. 14, 2002, HHS formally adopted these changes. In a press release accompanying the final modifications to the Privacy Rule, the Secretary of HHS, Tommy Thompson, commented on the change in the Department's position on the consent requirement, which created ''serious unintended consequences'' that would have interfered with patients' access to quality care. In this regard, Secretary Thompson noted: ''[t]he prior regulation, while well-intentioned, would have forced sick or injured patients to run all around town getting signatures before they could get care or medicine. This regulation gives patients the power to protect their privacy and still get efficient health care.''

III. Preemption

Preemption is a process for determining which law or rule controls when a federal and state law addresses the same or similar issue. With respect to the Privacy Rule, the preemption standard set forth in HIPAA contains several components. 42 U.S.C. § 1320d-7; 45 C.F.R. § 160.203. First, specific state public health and regulatory reporting laws remain unaffected by the Privacy Rule and continue in full force. 42 U.S.C. § 1320d-7(b), (c). For example, laws that provide for the reporting of disease or injury, or child abuse are not preempted. Second, HHS has the authority to deem certain enumerated types of laws ''not preempted,'' such as laws that are necessary to prevent fraud and abuse related to the provision of, or payment for, health care, and laws that are designed to regulate the manufacture, registration, distribution or dispensing of controlled substances. 42 U.S.C. § 1320d-7(a)(2)(A). Third, and more important here, the Privacy Rule does not preempt state laws that relate to the privacy of health information and are ''contrary to'' and ''more stringent than'' a provision of the Privacy Rule. 42 U.S.C. § 1320d-7(a)(2)(B).

''Contrary to'' means, in essence, that it is impossible to comply with both the federal and state law, or the state law stands as an obstacle to the accomplishment or execution of the purpose of the Privacy Rule. Given this narrow interpretation of ''contrary,'' it is rare that a state law will be truly ''contrary to'' a provision of the Privacy Rule, as both authorities are (almost always) permissive and, therefore, co-exist (as discussed below). ''More stringent'' is defined broadly based on six potential tests. Relevant to the issue of legal permission, ''more stringent'' means that a law provides the patient with greater privacy protection or, with respect to the form, substance, or the need for express legal permission from a patient, provides requirements that narrow the scope or duration, increase the privacy protections afforded (*e.g.*, expand the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, or restricts a use or disclosure. 45 C.F.R. § 160.202.

Effectively, the ''contrary and more stringent'' preemption standards create a ''federal floor'' upon which states may build more protective standards with laws and regulations. The result, as HHS noted, will be a ''patchwork'' of privacy protections that vary by state.

IV. Preemption of State Privacy Laws Pertaining to Consent

A. Overview of Preemption

Although the Privacy Rule no longer requires legal permission for TPO, state laws, in fact, may require legal permission for TPO and, under the preemption standard set forth above, these laws effectively will control.

States regulate health care providers in two principal (although certainly not exclusive) contexts. First, a number of state laws require a specific type of provider (*e.g.*, a hospital or physician) to obtain legal permission prior to disclosing health information, with certain exceptions. Common exceptions include those for treatment of a patient, payment or reimbursement for health care services, or for auditing or other activities that are similar to ''health care operations.'' However, exceptions for certain payment activities and certain types of health care operations may be narrower than defined under the Privacy Rule. Thus, legal permission still may be required for activities that otherwise would be permitted without legal permission under the Privacy Rule. Nowhere is this more prevalent than with respect to sensitive information, the second area of state regulation. Information related to specific conditions or illnesses, such as genetic test results, information on human immunodeficiency virus and other communicable or sexually-transmitted diseases, substance abuse records, and mental health information, is often afforded heightened protection under state law—generally in the form of restricted disclosures and detailed legal permission requirements. Accordingly, these laws may not only require legal permission for disclosures for payment and health care operations but also for treatment. We discuss several examples below.

B. Preemption Principles Applied to State Laws Governing Disclosure of Information for TPO

Health Care Operations of Another. In Texas, a hospital may not disclose any ''health care information'' about a patient without the patient's written authorization, except in 20 enumerated circumstances. Tex. Health and Safety Code § 241.152. This law permits disclosures without legal permission for most treatment and payment activities, and many health care operations. (In other words, many TPO-like disclosures are encompassed within the 20 exceptions.) However (unlike the

  HLR ISSN 1064-2137

Privacy Rule), the state law does not contemplate disclosures for the *health care operations of another* without legal permission. *Id.* § 241.153.

The Privacy Rule permits disclosures without legal permission for the health care operations of another in certain circumstances. Despite the difference between the state law and the Privacy Rule, the two authorities are not ''contrary'' because it is possible to comply with both (*e.g.*, both permit, *but do not require*, these disclosures). Therefore, the state law provision is not preempted, *per se*. As a result, as a practical matter, a hospital will need to comply with the ''more stringent'' provision in any particular instance. As applied to this situation, a hospital will be required to follow state law and obtain legal permission prior to disclosing health information for the health care operations of another entity, even though the Privacy Rule does not require any type of legal permission for such a disclosure.

Health Care Operations and Payment. In Colorado, ''all information obtained and records prepared in the course of providing services'' to the mentally ill are considered confidential and privileged. Colo. Rev. Stat. Ann. § 27-10-120. The information may be disclosed only in seven enumerated circumstances without legal permission. Pertinent here are disclosures (1) in communications between qualified professional personnel in the provision of services or referrals (*e.g.*, ''treatment''), and (2) to the extent necessary to make claims on behalf of a recipient of aid, insurance or medical assistance (regarding ''payment'').

The Privacy Rule permits disclosures without legal permission for the health care operations of another in certain circumstances. That said, the state and federal authorities are not contrary because it is possible to comply with both (*e.g.*, both permit, but do not require, these disclosures). Therefore, the state law provision is not preempted, *per se*. As a result, as a practical matter, a health care provider possessing mental health information will need to comply with the ''more stringent'' provision in any particular instance. As applied to this situation, it appears that legal permission will be required for disclosures for health care operations both of the holder and recipient, as none of the exceptions explicitly allow such disclosures without legal permission. Further, the disclosures permitted for payment are a subset of those permitted under the Privacy Rule. For example, utilization review activities and disclosures to consumer reporting agencies are not explicitly included in the exceptions in the Colorado law. For these payment activities (including those of the holder and recipient), legal permission will be required.

Treatment, Payment and Health Care Operations. Under New Jersey's Genetic Privacy Act, ''regardless of the manner of receipt or the source of genetic information, including information received from an individual, a person may not disclose or be compelled, by subpoena or any other means, to disclose the identity of an individual upon who[m] a genetic test has been performed or to disclose genetic information about the individual in a manner that permits identification of the individual,'' without authorization of the individual, except in nine enumerated instances. N.J. Ann. Stat. § 10:5-47. The exceptions are so narrow that the only permissible disclosures for ''treatment''-like activities include ''for the purpose of diagnosing relatives of a decedent'' and ''newborn screening.'' There are no permissible disclosures for ''payment'' or ''health care operations,'' absent authorization.

While the Privacy Rule permits disclosures without legal permission, the state and federal laws are not contrary because it is possible to comply with both (*e.g.*, both permit, but do not require, these disclosures). Therefore, the state law provision is not preempted, *per se*. As a result, as a practical matter, any provider in possession of the protected information will need to comply with the ''more stringent'' provision in any particular instance. As applied to this situation, it will require the holder of the information to obtain legal permission for most TPO.

V. Conclusion

Despite new leniency in the modified Privacy Rule's approach to consent, health care providers may be required under state law to obtain legal permission prior to disclosing health information for treatment, payment, and health care operations. This is particularly true where the health information at issue contains sensitive information, or the disclosure at issue is for the TPO of another entity. Review of state law will be critical in determining the precise restrictions on uses and disclosures.

BNA's Health Law Reporter is interested in publishing articles by health care practitioners and other experts on subjects of concern to the health care legal community, as well as reporting on significant settlement and pending lawsuits. If you are interested in writing an article, or alerting us to developments that might be of interest, please contact Susan Webster, the managing editor, at (202) 452 4220, email: swebster@bna.com, or submit your idea in writing to: Health Law Reporter, Bureau of National Affairs, Inc. 1231 25th St. N.W., Washington, D.C. 20037