HIPAA Privacy and Inter-Provider Disclosures: Responding to the Recalcitrant Provider

By Brian Gradle, Esq.

Among the unintended consequences of the HIPAA privacy rule arising since the rule's April 14, 2003 compliance date is the reluctance—or in some cases the refusal--of healthcare providers to provide protected health information (PHI) to other healthcare providers.

The reasons for this recalcitrance are manifold, including a general apprehension by some providers regarding the disclosure of PHI, confusion regarding the scope of permissible disclosures under the privacy rule, and a conscious decision by some providers to afford rights to patients regarding the disclosure of their PHI that exceed those mandated by the privacy rule.

It is essential that when faced with a "recalcitrant" provider—one who, for whatever reason, resists or refuses requests to provide PHI that is to be used for legitimate, appropriate purposes--that the requesting provider have in place a process for attempting to determine the concerns of the provider, and a means to address those concerns. As a preliminary matter, however, it is essential to understand what the *final* privacy rule says regarding such disclosures of PHI.

First, the privacy rule permits a covered entity to disclose PHI for the *treatment* activities of any healthcare provider (including providers that are not covered by the privacy rule, such as those that do not engage in electronic transactions). The privacy rule permits, for example, a primary care physician to send a copy of an individual's medical record, without the individual's authorization, to a specialist who needs the information to treat the individual. Likewise, the privacy rule permits a hospital to send a patient's healthcare instructions without patient authorization to a nursing home to which the patient is transferred. Health information can include such things as x-rays, lab and pathology reports, diagnoses, and other medical information.

Second, a covered entity may disclose PHI for the *payment* activities of a healthcare provider. For example, a hospital may disclose PHI to an ambulance service provider in order for the ambulance service to be paid for its services.

Third, a covered entity may disclose PHI to another covered entity (including providers that are covered entities) for certain *healthcare operations* of the covered entity, provided that both entities had a relationship with the individual, the information pertains to the relationship, and the disclosure is for certain prescribed purposes, such as quality

assessment or improvement, provider evaluation or training, or for healthcare fraud and abuse detection or compliance.

Importantly, disclosures of PHI for purposes of payment or healthcare operations are still subject to the privacy rule's "minimum necessary" requirements. In other words, the PHI that is disclosed must be the minimum amount that is necessary to accomplish the particular purpose for the disclosure.

Some of the confusion within the provider community regarding when PHI can and cannot be provided without patient authorization stems from the changes that were made between the December 2000 "final" privacy rule and the "modified final" privacy rule that was released in August 2002. Under the December 2000 version, healthcare providers with a direct treatment relationship with individuals (such as physicians, hospitals, and pharmacies) were required to obtain an individual's written consent prior to using or disclosing PHI for treatment, payment, or healthcare operations purposes. Consent was intended to be a one-time, general permission from the individual, which could be revoked.

In light of concerns that the government received regarding the consent provision for direct healthcare providers, the August 2002 modified final privacy rule eliminated the consent requirement and permits healthcare providers with a direct treatment relationship with individuals to use and disclose PHI without an individual's consent for treatment, payment, and healthcare operations. This modification was "partnered," however, with the requirement that direct-treatment providers must make a good-faith effort to obtain a written acknowledgement of receipt of the provider's notice-of-privacy practices. The intent of this modification is to preserve the patient's opportunity to raise questions about the privacy practices of the provider, without requiring patient consent.

Importantly, covered entities, if they wish to do so, can nonetheless implement a policy to obtain the consent of individuals prior to using PHI for treatment, payment, or healthcare operations purposes.

Providers should have a process in place for addressing the concerns of the recalcitrant provider—one who refuses or resists providing PHI upon a provider's request. Each provider should develop its own process for this type of situation. A provider might choose a process that follows this framework:

* When a request for a permissible disclosure of PHI under the privacy rule is refused, contact the provider's privacy official. The privacy official is responsible for the implementation and operation of the provider's policies and procedures, and should have the best understanding of the privacy rule within the provider's organization.

* Ensure that the provider understands the requirements and standards of the *final* privacy rule, and is distinguishing these requirements and standards regarding patient consent from those of the earlier version.
* Depending upon your reason for requesting the PHI (e.g., treatment, payment, or healthcare operations), clarify for the provider's privacy official why you are requesting the PHI, and the basis under which the PHI may be provided to you without requiring patient authorization.
* If the provider still refuses to provide the information, ask whether this is because of a more stringent state law provision (the privacy rule does not preempt such laws), or whether it is a policy decision made by the provider itself.
* To the extent it is required under state law, have your privacy official and/or counsel review the provision to confirm its applicability.
* If it is a policy decision, determine whether the policy reflects the provisions of the earlier privacy rule, rather than reflecting a conscious decision of the provider to create a heightened level of patient privacy. If it is a conscious decision, recognize that it is within the prerogative of the provider, and does not violate the privacy rule, to provide heightened protection for the patient.
* If the provider continues to insist that you obtain patient authorization to have PHI disclosed to you, make sure that the authorization form that you use is compliant with the privacy rule.

HIPAA is not intended to disrupt the flow of health information by and between healthcare providers for legitimate, routine purposes such as patient care, payment, and certain healthcare operations. Nevertheless, a significant amount of confusion remains regarding such disclosures. When confronted with a provider who resists or refuses to provide PHI for such purposes, take appropriate steps to determine the nature of the provider's concern, and to address the concern to the provider's satisfaction.

This article is designed to provide accurate and authoritative information with respect to its subject matter. However, it is provided with the understanding that neither the author nor the publisher is engaged in rendering legal or other professional services. If such legal or professional services are required, please seek the services of a competent professional.

Brian Gradle, Esq., is an attorney with Hogan & Hartson, L.L.P., Washington, D.C. He is a member of HFMA's HIPAA @Work Task Force. He can be reached at bdgradle@hhlaw.com.