

# Litigation

## *Disclosure of Protected Health Information For Legal Proceedings* HIPAA Privacy Regulations Make Use In Litigation a Cumbersome Task

BY LINDA MALEK  
AND STACEY GOLDSTON

NOW THAT the dust has seemingly settled around compliance initiatives under the Health Insurance Portability and Accountability Act (HIPAA), a range of unexpected implications of the HIPAA Privacy Regulations are being encountered by those inside and outside of the healthcare industry, specifically in the context of litigation. In many instances, these requirements protect individually identifiable health information to a greater extent than existing law, which has created additional constraints for entities wishing to use, disclose or acquire this information for legal proceedings.

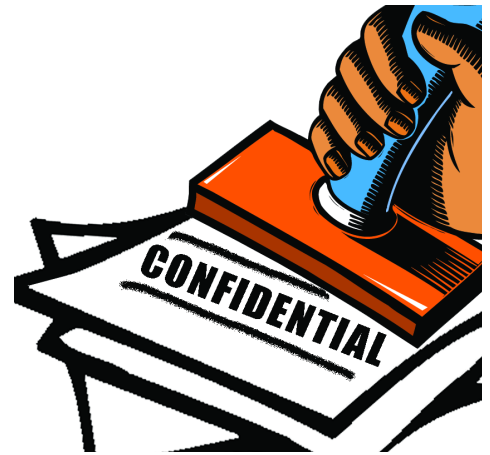
Promulgated by the U.S. Department of Health and Human Services (HHS) and in effect since April 2003, the Privacy Regulations seek to protect the confidentiality of health information by regulating its use and disclosure by covered entities. Covered entities are health plans, healthcare clearinghouses and healthcare providers that transmit health information in electronic form in connection with a standard transaction. While the Privacy Regulations are applicable only to covered entities, in the context of litigation the requirements as a practical matter also affect any entity that needs to secure health information from a covered entity. This article will explore the role of the Privacy Regulations in the use or

disclosure of protected health information (PHI) in litigation by covered and non-covered entities.

### Use in Litigation

Covered entities are generally permitted to use or disclose PHI that they create or obtain for their own healthcare operations. Included in the definition of healthcare operations is "conducting or arranging for legal services." HHS has not officially opined on the issue of whether or not litigation constitutes "conducting or arranging for legal services" within the meaning of the healthcare operations exception. However, in the absence of official guidance a reasonable interpretation of this language would arguably permit covered entities to use or disclose PHI in a lawsuit to which the entity is a party and is trying to defend itself.<sup>1</sup>

In all cases, the contemplated use or disclosure of PHI by a covered entity must be examined in light of the means by which the entity acquired the information. If a covered entity did not create the PHI but instead obtained it (or it was obtained on behalf of the covered entity) pursuant to a process that placed restrictions on its use or disclosure, these restrictions must be observed, and take precedence over the healthcare operations exception. For example, if a covered entity obtained PHI pursuant to an authorization, the use or disclosure of the subject information will be limited to the purpose for which the authorization was given as well as the expiration date or event contained in the authorization.



### Judicial Proceedings

If a covered entity creates PHI or obtains it in a manner in which the information is not subject to restrictions on its use or disclosure, the covered entity may arguably use this information for litigation purposes to defend itself pursuant to the healthcare operations exception. This includes disclosing PHI to a court and to other parties in the course of litigation in order to conduct legal services for the covered entity.

If a covered entity initially obtained PHI subject to restrictions, use or disclosure of this information is more complex. Certain restrictions will not prohibit a covered entity from using or disclosing PHI for litigation purposes so long as the intended use is permissible in light of the restrictions. In other cases, the restrictions are such that the subject information cannot be used or disclosed for litigation purposes in the absence of other measures that would enable the use or disclosure, such as obtaining an authorization, or following other requirements of the

Linda Malek is a partner at Moses & Singer and chairwoman of the firm's health practice. Stacey Goldston is an associate at the firm.

Privacy Regulations for the use or disclosure of such information, as described further in the next section.

The use or disclosure of PHI in an organized healthcare arrangement (OHCA) presents an example of a situation in which a covered entity may possess PHI subject to restrictions but which may also be permissibly disclosed in certain scenarios. OHCA's are arrangements or relationships between two or more covered entities that participate in joint collaborations and subsequently share PHI about individuals among one another in order to facilitate their joint operations. The Privacy Regulations recognize a number of different arrangements for both providers and group health plans that qualify as OHCA's.<sup>2</sup> A common example of an OHCA is a hospital where doctors employed by other facilities with medical staff privileges treat patients together with the hospital. In these situations PHI must be shared among the doctor(s) and the hospital in order to treat patients, receive payment for services and for healthcare operations activities.

The Privacy Regulations permit the disclosure of PHI by a covered entity that participates in an OHCA to any other participating covered entity for the healthcare operations of the OHCA.<sup>3</sup> As discussed above, conducting or arranging for legal services constitutes healthcare operations. However, in the context of OHCA's, the disclosure of PHI must be for the healthcare operations of the OHCA, not of any individual participating entity. This is another murky area under the Privacy Regulations with the potential for a number of different constructions; again, although HHS has not opined on this issue, one reasonable construction would appear to be that if the cause of action arises out of a function or activity performed by one or more members of the OHCA for, or on behalf of the OHCA, then defending the entity in resulting litigation would fall into the healthcare operations of the OHCA. Conversely, if the cause of action arose out of a function or activity completed independently of the OHCA by an

individual member of the OHCA, then defending the entity in the resulting litigation would not constitute the healthcare operations of the OHCA.

A prime example of a situation in which PHI acquired by a covered entity is subject to restrictions occurs when a covered entity acquires PHI pursuant to an authorization. If a covered entity possesses PHI obtained pursuant to a validly executed authorization it must be obeyed, and in doing so, the use or disclosure of the information will be restricted by the requirements set forth in the authorization despite the healthcare operations exception.

### **If Exception Does Not Apply**

As discussed earlier, the Privacy Regulations contain specific requirements with respect to the disclosure of PHI by covered entities. Although these requirements are the responsibility of the covered entity that maintains the PHI, entities requesting the information (whether covered entities or not), as a practical matter, must comply with these requirements in order to obtain the information. In other words, unless in making a request for PHI the entity seeking the information complies with the Privacy Regulations' requirements for the disclosure of PHI, the covered entity will be unable to respond to the request.

In circumstances where the healthcare operations exception does not apply, §164.512(e) essentially provides three methods for properly requesting PHI from a covered entity. The first method permits covered entities to disclose PHI in response to a court order directing the desired use or disclosure. The second method allows covered entities to disclose PHI when they receive a subpoena, discovery request or other lawful process along with "satisfactory assurances"<sup>4</sup> that the subject individual has been notified of the request. The third method permits disclosure when the requesting entity has provided the disclosing covered entity with satisfactory assurances that it has

expended reasonable efforts to secure a qualified protective order that prohibits the use or disclosure of the information for any purpose other than the proceeding for which it is requested, and requires that the information be destroyed or returned to the covered entity at the conclusion of the proceeding.

With respect to notifying the subject individual, "satisfactory assurances" constitute a written statement (and accompanying documentation) that the requesting entity has made a good faith attempt to notify the individual of the request; the notice contains information sufficient to notify the individual of the proceeding for which the information is being requested enabling the individual to raise an objection; and the time period during which the individual could have raised an objection has passed and no objection was filed or any that were filed have been resolved in a manner consistent with disclosure. A HIPAA-compliant authorization will fulfill this satisfactory assurances provision in terms of providing notice to the subject individual.

"Satisfactory assurances" that a reasonable attempt has been made to secure a qualified protective order amounts to a written statement (and accompanying documentation) that establishes that the parties to the proceeding have agreed to a qualified protective order, it has been presented to the tribunal responsible for the dispute, or the entity requesting the information has requested a qualified protective order from this tribunal.

### **New York State Law Issues**

Entities wishing to obtain PHI in New York state in the context of litigation have additional compliance requirements. With respect to the disclosure of PHI by a provider, New York state law is more stringent than, but not contrary to, the Privacy Regulations. The preemption guidelines under the Privacy Regulations state that when a state law is more stringent than, (i.e. gives greater protection to individuals) and contrary to (i.e. it would

be impossible to comply with both the state law and the Privacy Regulations) a provision in the Privacy Regulations, the state law applies. If a state law is more stringent than the Privacy Regulations, but not contrary to them, then both laws must be applied. Here, New York law is more stringent than the Privacy Regulations but it is not contrary and therefore both laws must be applied.

When an entity wishes to obtain PHI from a HIPAA-covered provider, the situation becomes somewhat complex. As stated above, state law preempts the Privacy Regulations only when the state law is both more stringent than, and contrary to, the corresponding provision in the Privacy Regulations. In this case, the applicable New York laws are more stringent than, but not contrary to, the Privacy Regulations and therefore both must be respected. However, depending on the type of provider from which the PHI is being requested, the procedure that must be followed under New York law differs.

CPLR §2302 sets forth the requirements for subpoenaing information from a patient's clinical record (essentially, the patient's medical record) maintained by an entity licensed or operated by the Office of Mental Health or the Office of Mental Retardation and Developmental Disabilities (OMH/OMRDD). This law requires that a subpoena that requests information contained in a patient's clinical record be accompanied by a court order. As a result, before PHI is requested from a New York provider, the requesting entity must ascertain whether the provider is licensed or operated by OMH/OMRDD and if so, a court order is necessary. A court order will also satisfy the requirements for disclosures for judicial and administrative purposes under §164.512(e) of the Privacy Regulations.

CPLR §3122(a) requires that a signed authorization accompany a subpoena when an individual's medical records are being sought from a provider. Unlike §2302, which is only applicable to providers licensed or operated by OMH/OMRDD, §3122(a) speaks to all

providers. Since §2302 is more restrictive and more specific in its application than §3122(a), §2302 is ostensibly applicable only with respect to providers licensed or operated by OMH/OMRDD and §3122(a) would be applicable to all other providers not covered by §2302. If PHI is to be obtained from a New York provider that is not a HIPAA covered entity, compliance with §3122(a) or §2302, as applicable, is all that is necessary.

There are more options for obtaining PHI from a medical provider as "defined" by §3122(a) than there are with respect to those subject to §2302. Assuming the disclosing entity is a HIPAA covered provider and is not otherwise subject to §2302, there are three ways in which to properly request PHI. First a court order can be secured. The second option is to serve a subpoena with a HIPAA-compliant authorization. This would be the best practice since it meets the requirements of §3122(a) and the Privacy Regulations. Finally, a subpoena can be served with a non-HIPAA compliant authorization that satisfies §3122(a) along with another process that otherwise meets the requirements of §164.512(e) of the Privacy Regulations. The latter option is a likely alternative in situations in which securing an authorization would be difficult. For instance, if an attorney is representing an individual in a will contest and is trying to access the health information of the deceased whose personal representative is also the adversary, it is unlikely that the attorney will successfully secure the authorization.

### Steps to Take

The Privacy Regulations have undoubtedly made the use of health information in litigation a more cumbersome task. Going forward, both HIPAA covered and non-covered entities will need to understand the intricacies of using, disclosing and obtaining PHI for legal proceedings. Before using, disclosing or requesting PHI, the following determinations must be made, in consultation with counsel, to ascertain whether the use or disclosure

is appropriate:

If an entity is a covered entity and it wishes to use or disclose PHI for litigation purposes, a determination must be made as to whether the PHI was created by the entity. If so, an analysis of the healthcare operations exception is appropriate to see if the PHI can be used or disclosed by the entity to defend itself. If the PHI was acquired pursuant to a process that further restricts its use or disclosure, such restrictions must be complied with.

If an entity is requesting PHI from a covered entity, the first determination to be made is whether the covered entity is a provider. If not, the Privacy Regulations must be followed in order for the covered entity to disclose the PHI.

If PHI is being requested from a covered entity that is a provider, the applicable New York law as well as the Privacy Regulations must be complied with.



(1) Although the healthcare operations exception may apply more broadly in the context of litigation, in this article we address its application only in situations where the entity wishes to use or disclose PHI to defend itself in litigation. Additionally, this article does not address circumstances where a joint defense agreement exists.

(2) Note that the Privacy Regulations place various requirements on OHCA's such as a requirement that notification of the existence of the OHCA be contained in the Notice of Privacy Practices of participating entities.

(3) The HIPAA Privacy Regulations do not preempt state privilege laws that are more stringent and contrary to HIPAA and in fact, in the preamble to the Privacy Rule HHS states that it does not intend to interfere with federal or state privilege laws. An analysis of such federal and state privilege laws is beyond the scope of this article.

(4) In all instances where a disclosure is permitted to be made by a covered entity upon receipt of satisfactory assurances, the covered entity must still comply with the minimum necessary rule contained in the Privacy Regulations and only disclose the minimum amount of PHI necessary to appropriately respond to the request.

This article is reprinted with permission from the April 5, 2004 edition of the NEW YORK LAW JOURNAL. © 2004 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact American Lawyer Media, Reprint Department at 800-888-8300 x6111. #070-04-04-0019