



hfma[™]

healthcare financial management association

UNANTICIPATED CHALLENGES OF THE HIPAA PRIVACY RULE

By Brian D. Gradle, Esq.

In the time preceding the HIPAA privacy rule's April 2003 compliance date, privacy officials and their staffs and counsel engaged in the painstaking process of anticipating and planning for the many issues arising from the privacy rule that could affect their organizations. Now, several months after the compliance date has passed, it is clear that despite such efforts, a number of unanticipated challenges have arisen that are demanding these privacy officials' attention.

Here are several of these concerns, as well as some strategies being employed by privacy officials to address them.

Heightened Patient Anxiety Over Privacy Practices

Contrary to its intended purpose, the delivery to patients of a notice of privacy practices has increased, rather than decreased, the anxiety level regarding the use and disclosure of health information. This phenomenon typically occurs among those who, prior to reading the notice, were generally unaware of the already permissible disclosures that hospitals, physicians, insurance companies, and other covered entities can make regarding health information.

As a result of such anxiety, and also as a result of the relative complexity of many notices, many privacy officials are finding that a significant amount of time is being spent responding to patient inquiries regarding the meaning of the notice. This is most typically seen in provider settings, such as physician offices and hospitals, where the individual, upon being asked to sign an acknowledgement of receipt of the notice, is more likely to review and consider the document.

In some cases, the use of a "layered approach," in which a summary of the notice is also presented to the patient, has been successful in addressing the more frequently asked questions, thereby reducing the administrative burden of answering individuals' questions.

Confusion Over Rights of Minors

Providers serving pediatric patients have particularly experienced heightened concerns of parents and legal guardians over the limitations that *state law* might impose upon their rights to view the medical records of their children. Although the HIPAA privacy law did not create these rights, the articulation of minors' rights in the notice of privacy practices has been a revelation for many parents and guardians.

State law may prohibit or restrict a physician from informing the parent of the child's medical condition without the child's consent, particularly regarding health information relating to such things as mental health, substance abuse, sexually transmitted disease, and teen pregnancy. It is therefore more important than ever that all covered entities understand the specific state laws that apply to the disclosure of minors' protected health information to parents and guardians. Moreover, no covered entity – particularly providers that are licensed and work in more than one

state – should ever assume that the regulations in one state are the same as those in another state.

An Unclear Role of Patients' Personal Representatives

Similar to the renewed focus on the rights of minors, covered entities have increased concerns over the role of people acting as “legal representatives” of patients. Although adult children, relatives, and close personal friends have served as informal counselors and confidantes of patients for years, the privacy rule has created new reasons for covered entities to verify the actual, lawful authority of such representatives to act on behalf of patients and receive protected health information.

For example, a “power of attorney” is frequently quite limited in its scope. It could be written, for example, to concern only matters regarding a person’s financial investments, and indeed might not grant any authority to an individual to receive a patient’s health information. Similarly, an adult child may be listed on an advanced directive as the person to make the decision regarding the cessation of life support, but that authority may be strictly limited to the situations articulated in the advanced directive.

Consequently, it is essential that before disclosing protected health information to any purported legal representative, a covered entity must clearly understand the true, legal authority of that individual under applicable law.

Another approach that some providers, particularly hospitals, have taken is to require patients to sign a “designated party release” form on admission. Such a release expressly authorizes the provider to discuss the patient’s condition with the people designated on the release, thereby avoiding the ambiguity that may arise if the hospital were only to obtain the oral permission, as required under the privacy rule.

Enhanced Disclosure Standards

Many healthcare entities are experiencing unexpected treatment and administrative delays because referring providers have chosen to adopt policies that exceed the privacy rule standards. Whether such heightened standards is a consequence of a desire to enhance patient involvement, or is a risk management device used because of uncertainty about the requirements of the privacy rule is not always clear.

For example, notwithstanding the fact that HIPAA permits, without patient authorization, provider-to-provider disclosure of health information for purposes of treatment, some providers have nevertheless determined that they will not make disclosures unless they have obtained prior patient authorization – in some cases requiring written patient authorization.

Providers that have tried to get protected health information from another covered entity for treatment purposes, only to be told that such information cannot be provided without the patient’s authorization, have sometimes found it effective to discuss the issue with the provider’s privacy official, in order to ensure that there is no misunderstanding of the permissible disclosure provisions of the privacy rule.

Once providers have been identified who insist upon written disclosure authorizations, providers seeking the information can consider taking steps to get the authorizations themselves, if necessary, to minimize treatment or administrative delays.

State Preemption Analysis

A continuing issue, although perhaps less unanticipated as the ones highlighted above, is the need to reconcile state law requirements with that of the federal privacy rule. What appears to be emerging as a result of such analyses is the view that most state privacy laws do not run contrary to the HIPAA privacy rule. Broadly speaking, a covered entity should continue to operate in accordance with the state statutes that it followed prior to HIPAA. Of course, it is still important to compare state laws and the HIPAA privacy rule, and to reconcile any provisions that overlap or appear to conflict.

Organizations should consult with their state professional associations and state regulatory agencies to determine whether appropriate preemption analyses are available.

Organized Health Care Arrangements

Many providers that serve on the medical staff of a hospital or other facility find themselves subject to two or more sets of privacy policies and procedures: one or more sets at the facility where they serve on the medical staff as part of an organized health care arrangement (OHCA), and the set that they have established in their own practice. Such providers must know the differences between such policies and procedures, and operate in accord with the appropriate set in the applicable setting.

Frequently, for example, covered entities have taken different approaches to disclosures that are permitted, but not required, under the privacy rule, such as the example described above where a provider requires patient authorization before disclosing health information to another party, even for treatment purposes.

Another common example relates to disclosures to law enforcement personnel. While such disclosures (under certain circumstances) are permissible under the privacy rule without the authorization of the individual, some covered entities have incorporated enhanced standards into their procedures that result in greater protection for the privacy of the individual in such situations.

Consequently, providers that are subject to more than one set of privacy policies need to ensure that they have an understanding of the differences between the two. Likewise, privacy officials affiliated with an OHCA should likewise take steps to inform their providers of the standards associated with that OHCA, particularly to the extent that the OHCA has adopted standards stricter than those required under the HIPAA privacy rule.

Business Associate Agreements

Finally, notwithstanding their efforts to resolve issues regarding the disclosure of protected health information to third parties, many covered entities continue to have HIPAA compliance issues surrounding the terms of business associate agreements. Frequently, these problems involve the inclusion of business terms that are not required under the HIPAA privacy rule but that are common components of commercial contracts.

Debate over whether to include these terms (for example, whether the parties will indemnify each other in case of mistakes, or whether one party will provide insurance for the other party) can sometimes delay the signing of BA agreements.

Notwithstanding any issues related to the negotiation of business terms, it is essential that covered entities always keep in mind that they, and not the business associate, bear the responsibility of entering into such contracts and for ensuring that the contracts contain, at a minimum, the required elements provided within the privacy rule.

About the Author

Brian Gradle is Counsel at Hogan & Hartson LLP in Washington, D.C., and a member of HFMA's HIPAA@Work Task Force. He may be reached at BDGRADLE@HHLAW.COM.

This article is designed for information purposes only and should not be considered legal advice.

*Copyright 2003 Healthcare Financial Management Association, all rights reserved.
www.hfma.org. Hogan & Hartson LLP has received permission to redistribute this document.*