HIPAA

What is the "Minimum" in Minimum Necessary?

by Susan W. Berson, J.D.

In August, the Department of Health and Human Services (HHS) released what we hope is the *final* set of modifications relating to the Standards for Privacy of Individual Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Now, the hard work begins.

Health care providers only have until April 14, 2003, to comply with the very complex requirements of the HIPAA privacy rules. Providers need to carefully review the rules and establish clear policies and procedures in their practices that meet HIPAA's "minimum necessary" requirements before that date.

The privacy rules state that covered entities, including providers, must make reasonable efforts to limit the use, disclosure, or receipt of protected health information (PHI) to the minimum necessary use, disclosure, or receipt that accomplishes the intended purpose of the request for such information. The minimum necessary requirement does not apply in certain circumstances (such as disclosure for treatment purposes); but covered entities can expect to regularly encounter situations where the minimum necessary requirements will need to be addressed.

While the proposed privacy rules mandated that a covered entity must evaluate each separate use or disclosure of PHI for minimum necessary issues, the final rule requires that a covered entity implement only general policies and procedures addressing minimum necessary uses and disclosures. This means that covered entities will not need to review and/or approve every use or disclosure on an individual basis. In the case of routine disclosures, covered entities will need to implement policies and procedures that restrict staff members' access to and use of PHI based on the needs of their specific roles or functions in the workplace. In the case of non-routine disclosures, a covered entity will need to establish criteria that can serve as guidelines for determining, on a case-by-case basis, whether a disclosure is permissible.

The first step in creating policies and procedures that comply with HIPAA's minimum necessary requirement is to conduct a privacy assessment. Covered entities need to understand how PHI flows throughout their organization before they can determine who needs access to what information for what purposes. Covered entities should review their operational functions and establish appropriate protocols for the disclosure of information related to each function.

For example, a protocol should be established for scheduling operating room time. While the people responsible for scheduling must have the necessary information to arrange for the appropriate time and equipment, they should not have access to patient information that is not relevant to scheduling. Similarly, while a covered entity may allow its entire staff access to a patient's medical record for treatment purposes, the treatment staff should not have access to the patient's financial information, which is not relevant to treatment.

In order to implement the minimum necessary privacy requirements, covered entities will need to add security measures not currently in place, such as locked file cabinets or records rooms and the separation of certain types of PHI so that it can only be accessed by designated members of the staff.

While meeting the minimum necessary privacy requirements means that covered entities must develop a significant number of new policies and procedures and redesign some of their internal work systems, the final modifications do ease some provider burdens. The final rule now explicitly permits certain incidental uses and disclosures that occur during a use or disclosure that is otherwise permitted. For example, a physician may now discuss a patient's treatment with a nurse at the nursing station and not worry about violating the privacy rules if a passerby or a person waiting in the office overhears patient information. These uses and disclosures will not be viewed as violations of the privacy rules as long as the covered entity has applied "reasonable" safeguards and implemented the minimum necessary standards. In this example, as long as the information the physician is disclosing to the nurse is the minimum necessary under the circumstances and they are speaking in appropriate voices, no violation will have occurred.

Because covered entities have only a few more months before they must comply with the HIPAA privacy rules, they should already be assessing how information is used and disclosed throughout their organization. The results of these inquiries will help them establish appropriate protocols and systems to comply with the complex minimum necessary requirement of HIPAA, and ensure that safeguards are in place to protect against inappropriate uses and disclosures.

Susan W. Berson, J.D., is a partner with the Washington, D.C., law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC.