HIPAA PRIVACY: THE NEXT STEPS FOR COVERED ENTITIES

The final privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") are here to stay. On December 28, 2000, the U.S. Department of Health and Human Services ("HHS") published final regulations that established privacy standards for personal health information. After some delays, HHS allowed the controversial regulations to go into effect unchanged on April 14, 2001. Most covered entities, including hospitals, HMOs, physicians, insurance companies and health plans are required to comply with the new rules by April 14, 2003.

The requirements set forth in the final regulations are extensive and create a compliance challenge that can be compared to a broader and more expensive version of Y2K. Compliance with the final regulations is not simply an information technology issue. Rather, compliance not only requires covered entities to make sure their software is HIPAA compliant and addresses requirements under the regulations such as access, monitoring and auditing, but also requires covered entities to enter into agreements with entities with whom they share protected health information, implement limitations on how they use protected health information and develop and use certain forms and privacy policies.

Now that the regulations appear to be here to stay, despite vocal opposition, most covered entities need to take steps to ensure that they are in compliance by April 14, 2003. If it sounds far away, remember the time it took your organization to prepare for Y2K? Consider that Y2K preparation was for a single moment in time, while compliance with the privacy regulations requires organizational changes that will last indefinitely.

This article briefly reviews the privacy regulations and outlines the steps covered entities should take as a result of the privacy regulations. Note, however, that the privacy regulations apply in total to covered entities regardless of size. As a result, it is impossible to present a blueprint that is effective for all covered entities. Instead, this article describes issues and approaches that likely will apply to all covered entities. It is important that each covered entity conducts its own self-assessment to determine what compliance steps are necessary for the entity.

History of Privacy Regulations

In 1996, Congress called for steps to improve the efficiency and effectiveness of the health care system by encouraging the development of standards and requirements for the transmission of certain health information. This gave rise to certain Administrative Simplification provisions of HIPAA, including the requirement that Congress enact privacy legislation by August 1999 and, if it failed to enact appropriate legislation, HHS was required to issue rules establishing privacy standards.

The final regulations accomplish several objectives. First, they establish the standards for the use and disclosure of protected health information by covered entities and their business associates. Second, they establish consent and authorization requirements for otherwise using protected health information. Third, the regulations require covered entities to establish privacy
practices and provide patients and beneficiaries with notices of such privacy practices. Fourth, the regulations permit individuals to access, obtain an accounting of, and amend their own health information.

The regulations apply to "covered entities," which include health care providers, health plans and health care clearinghouses who transmit health information in electronic form in connection with standard transactions such as claim submission and eligibility requirements. Information protected by the final regulations, which is generally referred to as "protected health information" or "PHI," includes individually identifiable health information that is transmitted or maintained in any form or medium concerning an individual's past, present or future physical or mental health or condition, whether it relates to the provision of health care to the individual or the payment for the provision of health care to an individual.

Generally, providers having a direct treatment relationship with an individual are required to obtain the individual's consent before using PHI for treatment, payment and health care operations. The regulations permit a covered entity to make certain disclosures without an individual's consent in the interest of public policy, including disclosures for law enforcement purposes, research and public health activities. An individual's PHI may not be used by a covered entity for any other reason without obtaining the individual's express authorization to such use of the PHI.

Unless the disclosure of PHI is being made for treatment purposes, a covered entity must make reasonable efforts to limit its use or disclosure of or request for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. While this typically requires an evaluation of the use or disclosure of the PHI on a case-by-case basis, the final rules permit a covered entity that makes disclosures of or requests for PHI on a routine and recurring basis to implement policies and procedures limiting the PHI disclosed or requested to amounts reasonably necessary to achieve the disclosure's purpose.

The regulations also require a covered entity to obtain "satisfactory assurance" from each business associate before the covered entity can disclose PHI to the business associate. A business associate is a person or entity that provides services on behalf of or to the covered entity where the services involve the disclosure of individually identifiable health information. Business associates will typically include billing companies, accounting firms, law firms, consulting firms and many other entities depending upon the operations of the covered entity. As will be discussed below, covered entities will have to enter into a business associate agreement or obtain other contractual assurances before disclosing PHI to a business associate.

Under the final rules, individuals have the ability to access and amend their PHI, as well as obtain an accounting of PHI disclosures made by a covered entity. Also, to protect PHI, covered entities are required to comply with numerous administrative requirements. These include appointing a privacy officer, adopting appropriate privacy policies, training workforce members on those policies and procedures, implementing safeguards to protect against improper uses or disclosures of PHI, and establish a process by which an individual may make a complaint to a covered entity regarding the entity's policies and procedures related to PHI.
Civil and criminal penalties could result if the regulations are violated. The Office of Civil Rights has been designated by HHS to enforce the regulations. At this point, the enforcement mechanisms are unclear. It is anticipated that both HHS and the Office of Civil Rights will issue guidance regarding various aspects of compliance with the privacy rules and enforcement of the privacy rules prior to April 14, 2003.

**Action Steps Each Covered Entity Should Take**

As stated previously, compliance with the privacy regulations extends well beyond information technology issues. While information technology is certainly a major part of HIPAA compliance, a covered entity cannot comply with HIPAA simply by purchasing a software package. Rather, compliance involves developing organizational security policies, procedures and standards, appropriate consent and authorization forms and taking the appropriate administrative steps required under the final rules. Following is a list of steps each covered entity should take to comply with the privacy regulations.

1. **Appoint a Privacy Officer.** A covered entity should appoint someone within the organization who is well-versed in the privacy regulations to lead the entity's assessment of its activities and implement necessary compliance steps. Depending on the organization's size, a privacy task force should be established to assist the compliance leader through the risk assessment process. It may be appropriate for certain complex entities or entities who do not have the expertise within the organization to engage an outside advisor to assist the self-assessment and compliance effort.

2. **Determine the Entity's Position Along the Compliance Trail.** Each covered entity should, as early as possible, begin evaluating the steps the covered entity needs to take in order to comply with the privacy regulations. It is important to know and understand the entity's current privacy practices so that new policies and procedures are integrated with existing practices. It also reveals the work necessary for an organization to become compliant, which allows the organization to assign appropriate personnel and establish a budget for compliance activities. While the compliance date remains some time away, the organizational change that will be required for many covered entities is tremendous. Therefore, it is never too early to begin.

3. **Identify Current Uses of PHI.** A covered entity should identify how it uses PHI. For instance, virtually all health care providers use PHI for treatment and payment purposes. However, it is important that the covered entity identify how it uses PHI for activities that would require a patient authorization rather than a patient consent. Identifying all of a covered entity's uses of PHI allows the covered entity to develop the appropriate forms and conduct the appropriate training to comply with the privacy regulations.

4. **Develop Appropriate Forms and Policies.** A covered entity should develop appropriate consent and authorization forms, as well as appropriate privacy policies and procedures. Because the privacy regulations require organizational change, the sooner a covered entity can develop these policies and procedures and begin testing them to ensure that they are compliant and best fit within the entity's current practices, the more likely a
covered entity will be in full compliance by the compliance date. This will also help minimize any disruption.

5. **Identify Business Associates.** One of the more arduous tasks for many covered entities will be to identify business associate relationships that require new or amended contracts. It is important that once business associates are identified, each agreement with the business associate be reviewed to determine how best the requirements set forth in the privacy rules can be integrated into the existing agreement with the business associate. If there is no existing agreement, the covered entity must enter into an agreement with the business associate that meets the requirements set forth in the final rules relating to the use of the PHI by the business associate. Any contracts with business associates entered into from this point should address the privacy regulations in some form. A covered entity that takes affirmative steps to deal with its business associates from the beginning will avoid the situation of having to amend an agreement at the last minute, which may affect the business terms of the agreement.

6. **Educating the Workforce.** Finally, a covered entity must consider how it will educate its employees on the privacy rules and the policies the covered entity will take to comply with the rules. Many health care providers have already experienced this education and training dilemma when implementing corporate compliance programs. Similar to such training, employees only need to be trained to the extent they interact with PHI. Therefore, training can be customized for various departments.

**Conclusion**

Compliance with the privacy regulations is certainly a time-consuming and expensive task. Because of the scope of the final rules, it is important that a covered entity begin evaluating the steps it must take to comply with privacy regulations as early as possible. Along the way, it is anticipated HHS will issue certain guidance for covered entities to comply with the rules. In the meantime, it is essential for covered entities to evaluate their current privacy practices and the necessary steps to become HIPAA compliant.

*By Steven A. Eisenberg, Esq.*
*BAKER & HOSTETLER LLP*
*COUNSELLORS AT LAW*