On August 14, 2002, the U.S. Department of Health and Human Services (“HHS”) issued the much-anticipated final Standards for Privacy of Individually Identifiable Health Information (the “Privacy Rule” or the “final rule”) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The HIPAA Privacy Rule is aimed at protecting confidential health information from being disclosed by “covered entities,” which include health care providers, health plans, and health care clearinghouses. The Privacy Rule was originally published by HHS in December 2000 (“the original rule”) and most covered entities must comply with the rule’s terms by April 14, 2003. A more detailed summary of the final Privacy Rule will be provided in the near future. Additional information can be found at http://www.hhs.gov/ocr/hipaa/whatsnew.html.

The final rule largely adopts modifications proposed at the end of March 2002 (the “proposed modifications”) that were designed to strengthen the original rule’s privacy protections without hindering patients’ access to health care. Based on comments received after issuance of the original rule and the proposed modifications in March 2002, HHS revised several key areas of the Rule, including the following:

**Consent and Notice of Privacy Practices**

The most significant change from the original Privacy Rule is the removal of the consent requirements for disclosures of protected health information (“PHI”) connected with routine health care delivery purposes — any treatment, payment or health care operations (“TPO”). Covered entities will need to provide patients with a notice of the provider’s privacy practices and the patient’s privacy rights, and do their best to obtain a written acknowledgement from the patient of receipt of such notice. Obtaining formal consent is optional, but encouraged, under the final Privacy Rule. The final rule does not modify the content requirements for this notice, which under the original final rule require providers to describe in specific detail their planned uses and disclosures of health information. The preamble of the final rule provides for the use of a “layered notice” — a short, summary notice that is placed on top of a longer notice containing all the required elements of the notice. The privacy notice must be provided at the time of first service delivery, except in emergency treatment situations or where otherwise impractical, but providers are required to attempt to obtain the acknowledgement as soon as practicable thereafter. Other covered entities, such as health plans, would not be required to obtain this acknowledgement.

HHS has emphasized that covered entities may voluntarily obtain patient consents as “an integral part of the ethical and other practice standards for many health care professionals” and that entities have “complete discretion” in designing their consent process.

The final rule allows for certain disclosures by covered entities to other covered entities for the treatment, payment, or certain operational purposes of the other covered entity, or for treatment purposes to health care providers, regardless whether they are covered entities, without consent or authorization if (1) both the disclosing and the receiving entities have a relationship with the individual whose information is being exchanged; and (2) the PHI pertains to the recipients’ relationship with the individual. If these two criteria are met, PHI may be disclosed for operational purposes of the covered entity, such as quality assessment, accreditation, licensing, credentialing, case management, training, or activities relating to improving health care or reducing health care costs, or for the purposes of detection or compliance with fraud and abuse laws.
Authorization

The final rule does not alter the original Privacy Rule’s requirement that covered entities obtain patient authorization for uses of patient information beyond TPO, but it does permit the use of one form of disclosure, rather than the several different forms required by the original rule. The final rule requires that all authorizations contain the following: (a) a description of the information to be used or disclosed; (b) identification of the persons or class of persons authorized to make the use or disclosure of the PHI; (c) identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure; (d) a description of each purpose of the use or disclosure; (e) an expiration date or event; (f) the individual’s signature and date; and (g) if signed by a personal representative, a statement of the personal representative’s authority to act on behalf of the individual.

All authorizations are required to contain the following notifications: (a) a statement that the individual may revoke the authorization in writing, and either a statement of the individual’s right to revoke and instructions on how the individual may revoke the authorization or a reference to the covered entity’s notice of privacy practices; (b) a statement that treatment, payment or other benefits may not be conditioned on the execution of the authorization, if this prohibition applies under the Privacy Rule, or, if the prohibition does not apply, a statement of the consequences of refusal to execute the authorization; and (c) a statement that PHI may be redisclosed by the recipient.

Minimum Necessary Rule

The original Privacy Rule required providers to adopt policies and procedures to safeguard and limit disclosure of the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. While this requirement remains in effect, the final rule clarifies that a provider could discuss a patient’s treatment with other professionals involved in the patient’s care without fear of violating the rule if they are overheard. The final rule further clarifies that incidental uses or disclosures that are the byproduct of an otherwise permissible use or disclosure do not violate the regulations, if the provider otherwise meets the minimum necessary rule and takes “reasonable safeguards” to avoid being overheard. Therefore, processes or conduct such as a patient sign-in sheet in a doctor’s office waiting room, keeping patient charts at their bedside, or doctor’s conferring with others at a nurse’s station can continue without fear of violating the rule.

Business Associates

Under the original and final Privacy Rule, third parties who may receive PHI from covered entities in the course of providing certain defined services for, or functions on behalf of, covered entities are defined as business associates. Covered entities are required to enter into a contractual agreement with business associates to safeguard the PHI shared with the business associate. The final rule allows most covered entities (except small health plans) to operate under existing contracts with business associates for up to one year beyond the April 14, 2003 compliance date of the Privacy Rule. This extension does not apply to oral contracts or other arrangements not reduced to writing and new written contracts entered into after April 14, 2003.

HHS also provides model language for business associate contracts to assist covered entities in compliance with the business associate provisions of the Privacy Rule. Importantly, these sample provisions are not necessarily sufficient to form a complete and binding contract. The parties to these agreements may wish to include other contractual provisions not required by HIPAA, such as indemnification and limitation of liability clauses, in order to allocate the risk associated with the use and disclosure of confidential patient health care information.

Medical Research

The final rule allows researchers to use a single combined form for both HIPAA and informed consent purposes, and modifies other provisions to more closely track (but still not supersede or preempt) the requirements of the so-called “Common Rule” and Food and Drug Administration regulations, both of which govern federally-funded research. As a result, the final rule, while reducing complexity, does not alter the basic requirement that those involved in medical research comply with multiple and overlapping sets of federal (as well as more stringent state) regulations relating to their work. The final rule permits the creation and dissemination of a limited data set (that
does not include directly identifiable information) for research, public health and health care operations. The final rule conditions disclosure of the limited data set on a covered entity and the recipient entering into a data use agreement (much like a business associate agreement). In the agreement, the recipient would agree to limit the use of the data set for the purposes for which it was given and to ensure the security of the data. In addition, the recipient would agree not to identify the information or use it to contact any individual.

**Marketing Materials**

Under the final rule, the use or disclosure of a patient’s PHI for a “marketing” communication requires an authorization by the patient. This change is more restrictive than the original rule, which allowed marketing without authorization if certain disclosures were made and patients were given the change to “opt out” of receiving marketing communications. However, the final rule does not impair the ability of providers and other covered entities to discuss treatment options with patients or to provide patients other health-related information concerning wellness programs, prescription refill reminders, and appointment notifications. As with the original rule, no authorization is required if the communication takes the form of a face-to-face encounter or a promotional gift of nominal value. The final rule also modifies the definition of marketing to clarify that it is the language of the communication itself (not the intent of the covered entity) that matters in determining whether a communication is marketing. Thus, under the final rule, a communication about a product or service is marketing if it "encourages recipients of the communication to purchase or use the product or service," unless the communication is made for certain enumerated purposes.

**Parental Access**

The original Privacy Rule may have unintentionally limited parents’ access to their child’s medical records. The final rule clarifies that state law, or other applicable law, governs in the area of minors and parents. Generally, the final rule provides parents with new rights to control the health information about their minor children, with limited exceptions based on state or other applicable law or professional practice.

**Other Modifications and Clarifications**

The final rule also revises and clarifies other provisions of interest of the Privacy Rule, including the following:

**Sale of Business:** The final rule amends the definition of “health care operations” to clarify HHS’s intent to permit the transfer of records from one covered entity to another upon a sale, transfer, merger or consolidation of all or part of the covered entity. The intent of this change is to resolve an ambiguity created under the original December 2000 rule concerning whether a selling entity could actually transfer records containing PHI upon the completion of a transaction, or whether such information could only be disclosed as part of due diligence.

**Accounting of Disclosures:** The final rule eliminates the requirement that a covered entity account for disclosures pursuant to a patient’s authorization (on the theory that the patient already knows about the disclosure if he or she has authorized it), incidental disclosures, or disclosures that are part of a limited data set. The Privacy Rule provides a simplified alternative approach for accounting for multiple research disclosures that includes providing a description of the research for which an individual’s PHI may have been disclosed and contact information.

**Disclosures for Treatment, Payment, or Health Care Operations of Another Covered Entity:** The final rule clarifies that covered entities are permitted to disclose PHI without consent or authorization for the treatment, payment and certain health care activities of another covered entity.

**PHI: Exclusion for Employment Records:** The final rule clarifies that employment records maintained by a covered entity in its capacity as an employer are excluded from the definition of PHI. If, however, an employee’s PHI is created, received or maintained by a covered entity in its capacity as health care provider and not as an employer (i.e., hospital employee is a hospital patient), then the patient’s information would be protected PHI under the rule.
Comment

By and large, the final Privacy Rule is less burdensome for health care providers than the original rule issued in December 2000. Now that the final rule has been issued, compliance with the HIPAA Privacy Rule needs to be a priority for all covered entities and business associates as the effective date of April 14, 2003 draws near. Navigating the seas of these comprehensive regulations safely will be essential for all providers in the coming months.

For more information, please contact Robert Portman, Chair of the Firm’s Health Care Law Practice at rportman@jenner.com or call 202 639-6000.