

ALERT

GOVERNMENT REGULATION / HEALTH LAW

December 2000 Number 6

HHS Issues Final—and Substantially Revised—Privacy Rule

The Secretary of the Department of Health and Human Services (“HHS”) has released the final Standards for Privacy of Individually Identifiable Health Information. These standards implement the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). HHS received over 52,000 comments in response to its proposed privacy rule published last year, 64 Fed. Reg. 59918 (Nov. 3, 1999).

The final rule, like the proposed rule:

- limits the non-consensual use and release of protected health information;
- requires covered entities¹ to provide individuals with periodic notices describing the uses and disclosures made of health information and the individual’s rights with respect to those uses and disclosures;
- gives individuals the right to access their medical records and to know who else has accessed them;
- restricts most disclosure of health care information to the minimum needed for the intended purpose; and
- establishes new criminal and civil sanctions for violations of the rule.

Not surprisingly, given the number of comments received and the complexity of the regulation proposed, the final rule differs markedly from the proposed privacy rule in several fundamental respects. This brief analysis is designed to highlight some of the most important changes in the rule.

¹Under both the proposed and final rule, the term “covered entity” includes health plans, health care clearinghouses and health care providers who transmit any health information in an electronic form in connection with a transaction covered by the rule.

Scope

The final rule significantly expands the reach of the rule. The proposed rule applied to “protected health information” (“PHI”), defined as “individually identifiable health information” (“IIHI”) that was electronically transmitted or maintained by a covered entity. Once information had been maintained or transmitted electronically by a covered entity, the protections would follow the information in whatever form it exists, including paper records.

The final rule broadens its reach by extending the definition of PHI to all IIHI that is transmitted or maintained by a covered entity electronically or in “any other form or medium.” As a result, the rule now applies to paper and oral communications as well. Although the extension of the final rule to cover paper and oral communications is a significant expansion, the actual impact of this change will vary by covered entity. For large entities, such as hospitals and health plans, the impact may not be all that substantial because of the difficulty in segregating information that had been transmitted or maintained electronically from that which had not. As a practical matter, most large entities would likely have treated all IIHI as covered by the rule, regardless of whether it had, in fact, ever been maintained or transmitted electronically. For smaller entities, such as physicians’ offices, that do not currently maintain or transmit a large number of electronic medical records, this change will likely have a greater impact because it will mean that all IIHI will be covered by the rule.

Refinement of “Minimum Necessary” Standard

Perhaps the most important, and most administratively burdensome, change in the final rule pertains to the requirement that covered entities limit their use and

disclosure of PHI to the “minimum necessary” amount. Under the proposed rule, a covered entity was required to make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure. This standard did not apply to certain uses and disclosures, such as those made at the request of an individual to access his or her own PHI or those made by a health care provider to a health plan for audit purposes. The proposed rule required a covered entity, to the extent it was technologically possible, to make minimum necessary determinations *on an individual basis*.

The final rule significantly modifies the proposed rule’s implementation guidelines by providing different requirements based on whether the PHI activity is a “use,” a “request,” or “disclosure.” On the positive side, the final rule clarifies that providers need not limit their disclosures of PHI to the minimum necessary amount when making disclosures for treatment purposes. For *uses of PHI*, a covered entity must implement policies and procedures to identify the persons or classes of persons in the entity’s workforce who need access to PHI to carry out their duties, the category or categories of PHI to which such persons or classes need access, and the conditions that would apply to such access. These policies must limit access only to the identified persons and the identified PHI necessary to complete job responsibilities and satisfy the conditions of the activity. For *routine requests and disclosures of PHI*, a covered entity must establish policies and procedures that limit the disclosure of PHI to the amount and type reasonably necessary to achieve the purpose of the request or disclosure. In this context, individual review of each request or disclosure is not required. The aforementioned policies must identify the types of PHI to be disclosed, the types of persons (e.g. routinely hired business associates) who would receive the PHI, and the conditions that would apply to such access. For *non-routine requests and disclosures*, the covered entity must develop criteria designed to limit the PHI disclosed to that information necessary to accomplish the purpose for which the disclosure is sought. In this context, the covered entity must review each request or disclosure individually in accordance with these policies and procedures. The rule also states that disclosure of an entire medical record requires documented justification that the entire record meets the minimum necessary standard;

otherwise, such comprehensive disclosure presumptively violates the rule.

Although the final rule provides some increased clarity over the proposed rule, it continues to place significant administrative burdens on covered entities and will, at a minimum, force them to operate in a climate of uncertainty given the vagueness of the requirement. While the proposed rule would have required covered entities to make minimum necessary decisions on an individual basis when possible, the final rule will require a complex “mapping” of personnel to the specific categories of PHI that they must access to perform their job functions. Indeed, HHS has stated in the preamble to the final rule that one of the largest initial and ongoing costs to covered entities from the final rule will arise from compliance with the minimum necessary standard. While the rule has been scaled back slightly to allow the use of standard policies for routine activities and to require a covered entity to make “reasonable efforts” (instead of “all” reasonable efforts, as originally proposed) in limiting PHI to what is minimally necessary, there will still be significant administrative burdens and costs associated with making individualized determinations for non-routine uses and disclosures of PHI.

Providers, But Not Health Plans, Are Required to Obtain Consent for Treatment, Payment and Health Care Operations

In a significant change for providers, the final rule requires providers to obtain consent prior to using or disclosing PHI for treatment, payment or health care operations. Under the proposed rule, health care providers, health plans and health care clearinghouses were permitted to use or disclose PHI for the purposes of treatment, payment or health care operations without having to obtain individual authorization.

Under the final rule, covered entities still do not need to obtain *individual authorization* for these purposes. However, *health care providers* who have a *direct treatment relationship* with an individual must obtain *consent* from the individual before using PHI for the purposes of treatment, payment or health care operations (with limited exceptions). A health care provider may refuse to treat an individual who refuses to provide consent. Other covered entities (e.g., health plans, health care clearing-

houses and health care providers with an indirect treatment relationship) do not need to obtain consent for such purposes, but are permitted to do so in their discretion, so long as they comply with the consent requirements. The consent form must be in plain language and contain certain specified requirements. It must be accompanied by a notice that provides details on the covered entity's health information practices. A covered entity must document and retain any signed consent for six years. An individual may revoke his or her consent except to the extent that a covered entity has relied upon it. A health plan, however, may disenroll an individual that revokes his or her consent if the consent was sought in conjunction with the individual's initial enrollment in the health plan. Similarly, a health care provider may refuse to continue to treat an individual who revokes his or her consent.

Health Plans Will Contract With Business Associates, Not Business Partners

The final rule revises, primarily for the better, the business partner requirements. The proposed rule defined a business partner as "a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity." Under the proposed rule, a covered entity could not disclose PHI to its business partner without "satisfactory assurance," in the form of a contract containing a number of required provisions designed to bind the business partner to the restrictions applicable to covered entities, that the confidentiality of the PHI would be maintained. The proposed rule also stated that the business partner contract should specify that individuals whose PHI is disclosed under the contract are intended third party beneficiaries. Under the proposed rule, a covered entity was required to take reasonable steps to ensure that its business partners complied with these requirements. A material breach by a business partner would be considered a violation of the rule by the covered entity if the covered entity knew or *reasonably should have known* of the breach and failed to take reasonable steps to cure the breach or terminate the contract.

The final rule makes several significant changes. The rule now refers to a "business associate" rather than a "business partner" in order to be consistent with the final rule on transactions and code sets. The final rule also modifies

the relevant definition. Under the final rule, a business associate is: (a) a person who uses or discloses PHI to perform or assist in the performance of a function or activity on behalf of the covered entity or organized health care arrangement; or (b) a person who provides specified services to a covered entity or organized health care arrangement if the services involve the disclosure of PHI.²

"Satisfactory assurance" in the form of a written contract is still required under the final rule. While most of the business associate contract requirements have remained the same, some have been clarified and others have been eliminated.

1. The preamble clarifies that the contract need only specify general reasons for use or disclosure and types of persons to whom the business associate may make further disclosures.
2. Although a business associate is generally only able to use or disclose PHI in a manner allowed by the covered entity, the final rule recognizes two exceptions. A contract may allow the business associate to:
 - use and disclose PHI for its own management and administration; and
 - provide data aggregation services relating to health care operations.
3. The final rule provides that a business associate must return or destroy PHI at the termination of the contract only if "*feasible*." If such action is not feasible, the business associate must agree to extend preferred protections to PHI for as long as it retains the PHI.
4. The regulations no longer require that a third party beneficiary relationship be created under the contract for individuals whose PHI is disclosed.

The final rule also minimizes the requirements of covered entities to monitor their business associates' compliance with the privacy rule. Under the final rule, a covered entity that has knowledge of a "pattern of activity or practice of the business associate that constituted a mate-

² These specified services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

rial breach or violation” of the business associate’s contract, must take “reasonable steps to cure the breach or end the violation.” If such steps are not successful, the covered entity must terminate the contract, *if feasible*, or, if termination is not feasible, report the problem to the Secretary.

The final rule has infused the business associate contracting requirements with significantly more flexibility. For example, business associates can now perform data analysis using PHI from multiple covered entities and need not automatically return or destroy all PHI at the termination of the contract. Moreover, the changes made in the final rule appear to lessen the risk of liability on a covered entity’s part. The removal of the third party beneficiary language requirement relieves an important liability concern for covered entities and the revised standard for monitoring the actions of business associates should help attenuate the potential liability of covered entities.

Other Changes of Interest

The final rule differs from the proposed rule in several other significant areas, including the following:

- **Health Care Operations.** The final rule significantly expands and clarifies the definition of “health care operations” to clearly encompass disease management and wellness programs when done by health plans and/or providers. In response to concerns raised by hospitals, it also allows for the limited use of IIIHI for fundraising activities when done on the covered entity’s own behalf.
- **Marketing.** The final rule contains a definition of marketing while the proposed rule did not. The new rule makes clear that marketing *does not include* efforts to describe the services available from, or entities participating in, a provider or plan network, and certain communications pertaining to the management of an individual’s treatment. The final rule also states, *inter alia*, that for certain purposes authorization is not required to use PHI for a “face-to-face” marketing encounter with an individual.
- **New Sub-Classifications for Covered Entities.** The final rule adds several new sub-classifications of covered entities apparently designed to ease compliance for covered entities with multiple operations and/or distinct legal relationships. Thus, entities that operate

as “organized health care arrangements,” (e.g. integrated delivery systems) can, for certain provisions of the rule, comply as a single covered entity. “Hybrid entities” are a single legal entity whose primary function is not as a covered entity (e.g. an employer with an employee health clinic). The rule clarifies that only the health care component of the hybrid entity must comply with the rule. “Affiliated entities” are legally separate covered entities that may choose to designate themselves as a single covered entity for purposes of complying with the rule.

- **Research.** The final rule includes more comprehensive restrictions on the use of PHI for research purposes.

Conclusion

While the final rule has clarified some of the ambiguities present in the propose rule it is decidedly more expansive, complex and administratively burdensome to covered entities than the proposed rule. Compliance will require covered entities to examine virtually every aspect of their information practices, revise their contracts with business associates and modify their contracting procedures, draft new medical information policies and procedures, authorizations, notice and consent forms, and establish new administrative procedures that govern how they use and disclose IIIHI. While compliance will not be required for two years from the effective date (February 26, 2001), the complexity of the rule is such that all covered entities should begin to take immediate steps toward compliance.

The final privacy rule contains a substantial number of other provisions that will significantly impact the operations of covered entities. Please contact us further if you would like to discuss the final rule in greater detail.

Bruce M. Fried
bruce.fried@shawpittman.com - 202.663.8006

Jordana G. Schwartz
jordana.schwartz@shawpittman.com - 202.663.8201

Janice Ziegler
janice.ziegler@shawpittman.com - 202.663.9196

Copyright © 2000 by Shaw Pittman. All Rights Reserved. This publication is provided by Shaw Pittman for general information purposes; it is not and should not be used as a substitute for legal advice.