# Final Privacy Rule Puts Health Information in National Spotlight



*by Dan Rode, MBA, FHFMA*

Amid much fanfare that included a ceremony with AHIMA representatives as invited guests, the Department of Health and Human Services (HHS) released the HIPAA standards for privacy of individually identifiable health information on December 20, 2000. The rule was published in the *Federal Register* (vol. 65, no. 250, pp. 82462-82829) on December 28.

Compliance with the final rule will be necessary February 26, 2003, for healthcare providers and most health plans, and February 26, 2003, for health plans that qualify as "small."

This article presents a brief overview of the final rule. However, it is strongly recommended that HIM professionals read the rule itself. Copies can be obtained online at www.ahima.org or at the HHS administrative simplification site at http://aspe.hhs.gov/admnsimp/.

**Who's Covered by the Privacy Rule?**

Like other HIPAA regulations, the privacy rule applies to health plans, healthcare clearinghouses, and providers who transmit "any health information in electronic form in connection with a transaction covered under" HIPAA.

While this application seems simple enough, the rule itself details health plan relationships with other health plans, sponsors, and enrollees. Health plans will have to give considerably more attention to health information and their relationship with enrollees and patients in the future. The rule also addresses the role of clearinghouses and when they are or are not covered by the rule.

An important distinction of the final rule is that **it protects all medical records and other individually identifiable health information in any form**, whether communicated electronically, on paper, or orally. Healthcare providers are also not simply defined by whether or not they transmit information electronically, since they are included if their "business associates" perform such electronic transactions for them. Given that few providers have no health information in electronic form, the rule essentially covers all healthcare providers.

Once an entity is considered covered under the applicability section of the rule, all healthcare information, no matter in what format or medium, is covered. **The best way to comply with the rule is to consider all healthcare information as covered**. Trying to identify exceptions will be more costly than being inclusive.

The rule also defines "business associates"--formerly known as "business partners" in the proposed rule. While it appears that the oversight function in the proposed rule has been reduced, explicit contracts are still required to protect health information and institutions.

**The Final Privacy Rule**

This article will summarize the rule in the same order as it appears in the *Federal Register*.

**Preemption of State Law**

The rule defines a number of terms, including "contrary," "more stringent," and "state law." In general, **any part of the rule that is contrary to a provision of state law preempts the provision of the state law**. Exceptions include situations in which:

- the state has secured an exception determination from HHS

- the state law is more stringent than the rule
- the state law relates to the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention
- the state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or licensure or certification of facilities or individuals

**Complaints, Compliance, and Penalties**

Under the final rule, a person who believes a covered entity is not complying with the rule's requirements can file a complaint within 180 days, unless the time limit is waived.

To facilitate HHS's investigation of a complaint, covered entities must provide records and compliance reports, cooperate with complaint investigations and compliance reviews, and permit access to information. Penalties under HIPAA could go as high as $250,000 per violation and from one to 10 years of imprisonment. The director of the HHS Office for Civil Rights will administer the privacy regulation and ensure its compliance.

**Other Definitions**

The rule contains a number of definitions that go beyond those in the proposed notice. These definitions qualify data, clinical, and information terms, persons affected by the rule, and health operation activities and functions. For instance, the rule uses "covered functions" to mean "functions of a covered entity the performance of which makes the entity a health plan, health care provider, or healthcare clearinghouse." Some of the definitions, such as "payment," become requirements (in this case, for patient accounting functions) and require close attention.

**Use and Disclosure of Protected Health Information**

Essentially, a covered entity may not use or disclose protected health information except as permitted by the rule. However, there are generally exceptions for every function.

The rule sets a standard for "minimum necessary" for disclosing or requesting protected health information from another covered entity. **A covered entity is expected to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request**. The standard does not apply to disclosures to or requests by a healthcare provider for treatment, disclosures made to the individual who is the subject of the information, uses that are required by law, or uses that are required for compliance with the rule.

A covered entity can use "deidentified" information, and the rule details how this can occur. It also defines how and under what agreements a covered entity can allow a business associate to collect, aggregate, or have access to protected information.

The rule also details the use or disclosure of information associated with situations that might involve personal representatives, minors, emancipated minors, individuals who might be involved in situations of abuse, neglect or endangerment, and deceased individuals. These situations may be also covered by state laws, and they will need to be reviewed by counsel to determine their impact on an entity.

Because protected information exists outside of the traditional medical record, most, if not all, of an entity's employees will need training on what information can be shared with anyone outside of those designated in the rule. The rule also covers an entity's protections when information might be disclosed by whistleblowers or work force members who are victims of a crime.

**Organizational Requirements**

The rule discusses how it applies to situations where an entity may be hard to define or where more than one entity may be providing the services of a health plan or provider. Here, again, covered entities will have to again work with counsel to determine how the rule applies to their situation, and privacy officers and administrators will have to ensure that compliance is maintained as entity relationships change or evolve.

**Consents and Authorization**

The final rule introduces the concept of a patient or individual's consent to reflect concerns that the proposed rule did not require a consent for release of information. **The rule requires a general "consent" for use or disclosure of information for treatment, payment, and healthcare operations**. The consent should be obtained before treatment is provided, with exceptions. The rule also addresses:

- when functions can be carried out without consent
- when a provider can condition treatment on whether the patient agrees to the consent
- the content and form of the consent
- the nature of a defective consent
- how a conflict regarding a "consent" versus a "authorization" should be resolved

The rule applies to covered healthcare providers for the "use or disclosure to carry out treatment, payment, or health care operations,"

**A more specific "authorization" is required for a covered entity to use or disclose protected health information for purposes other than treatment, payment, or operations**. Specific attention is also given to the need for an authorization when the information under consideration is in psychotherapy notes.

In general, entities need to keep copies of all consents and authorizations and document situations where the appropriate document was not present for a release of the covered information. In addition, in most cases, the patient or their representative should receive a copy of the consent or authorization.

In covering situations where the individual may not have the opportunity to object, such as release of information to meet certain legal requirements, the entity is required, in some cases, to inform the individual that information has been released. Since some of these situations cover release of information in a HIM department, special attention will need to be paid to these requirements.

**Notice of Privacy Practices for Protected Health Information (subhead)**

The rule requires that **a notice of privacy practices for protected health information be given to all affected individuals**. While such a notice might be mentioned in a consent or authorization, it cannot be part of the consent or authorization itself.

While the notice requirements suggest something on the order of a brochure or pamphlet, they also seem to suggest that an covered institution might have to "post" the notice. (It is to be hoped that this requirement will be clarified in the future.) The notice must contain:

- the uses and disclosures of health information the covered entity permits under the rule, including examples
- whether the entity will be using information to contact individuals to provide appointment reminders, approved marketing information, fund raising, or information (in the case of health plans) that may be released to sponsors of the individuals plan
- the rights of the individual to request restrictions on certain uses and disclosures, receive confidential communications, inspect, copy, and amend protected health information, receive an accounting of disclosures of protected information, and receive a paper copy of the notice
- the complaint mechanism associated with this notice, consents, and authorizations
- any limits to the uses and disclosures the entity wishes to add

**Rights to Request Privacy Protection for Protected Health Information (subhead)**

The rule specifies that individuals are permitted to request that an entity restrict the uses or disclosures of protected health information about them to carry out treatment, payment, or operations and other permitted disclosures. Covered entities, however, are not required to agree to such restriction and must inform the individual of the consequences of such a restriction.

The rule also specifies how a provider might continue to deliver services in spite of such a restriction, when the provider has no choice but to continue to provide the service or release information required by law.

**Access of Individuals to Protected Health Information (subhead)**

The rule also covers situations in which a covered entity does not have to comply or in which compliance can be modified. It calls for specific denial processes and provides some control over access by a covered entity. Likewise, the rule is very specific as to how and when protected health information can be amended.

**Accounting of Disclosures of Protected Health Information (subhead)**

The rule specifies that an individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested. There are several exceptions to this accounting and reporting requirement, including the use of data internally by the entity and certain specified legal releases. The accounting does not include situations prior to implementation of the rule, unless otherwise required.

The accounting must include (again with some exceptions), dates of disclosure, the entity or person that received the information and their address, and a brief description of the information disclosed and of the purpose of the disclosure.

The entity must act on the request within 60 days of the request (there is some provision for a 30-day extension). Under some conditions, the entity can charge the individual for the accounting, but much of it can be obtained for free.

**Privacy Officer, Training, and Other Requirements (subhead)**

The rule requires that the entity designate a privacy official who is responsible for the development and implementation of its policies and procedures. There are no other conditions on who could fulfill this obligation. The entity must also designate a contact person to receive complaints. Information regarding the privacy official and the complaint mechanism must be included in the notice discussed above.

The covered entity is also required to train "all members of its work force on the policies and procedures with respect to protected health information required." Specific training requirements are listed and must be supported by documentation.

**Where Do We Go from Here?**

Implementation will be a considerable undertaking, depending on the size of an entity, its current practices, and how different those may be from those required by the rule. Some changes required by the privacy rule will be part of the changes mandated by the transaction and code set standards published previously, or the security rules that, at press time, had not been released.

It may also be an expensive undertaking to define policy, procedures, and systems needed to meet the new requirements. HHS indicates that conforming to the privacy rule may cost the industry more than $17 billon over 10 years.

Considering the rule's far-reaching impacts, then, healthcare organizations need to make sure they are proceeding correctly. Unlike other HIPAA regulations that address process and standards, the privacy rule also addresses what many will consider legal issues, terms, and preemption situations. For this reason, during implementation, organizations should engage legal counsel.

Furthermore, the privacy rule intersects with a variety of existing rules, statutes, and other legal requirements that will cause requests for exceptions (by states) or affirmation by the courts. How much of this will occur before the implementation deadline remains to be seen. Once implementation takes place, counsel will continue to be needed for any modifications that occur due to rule changes or case law.

As implementation moves forward, the public and consumer interest groups will be watching closely. It may be that patients will assume that the called-for policies and procedures will be in place much sooner than required. All healthcare entities should make certain that they have reviewed the privacy rule with legal counsel and are prepared to answer questions from the public.

***Dan Rode*** *is AHIMA's vice president of policy and government relations. He can be reached at* mailto:dan.rode@ahima.org.

**Article citation**:
Rode, Dan. "Final Privacy Rule Puts Health Information in National Spotlight." *Journal of AHIMA* 72, no.2 (2001): 32A-C.