Five Steps to Reading the HIPAA Rules (HIPAA on the Job)

Save to myBoK

by Margret Amatayakul, RHIA, FHIMSS

HIPAA's administrative simplification regulations appear to be anything but simple. Part of the Health Insurance Portability and Accountability Act of 1996, these provisions are intended to achieve efficiency and effectiveness and promote use of information systems. There are definitely benefits to be achieved. But the regulations' length, flexibility, and lack of specificity result in the not-so-simple task of having to interpret the rules and make business decisions about how to implement the requirements.

Why Should I Read the Rules?

Why read the rules at all? After all, many publications and conferences provide information about HIPAA. But these other resources typically cannot cover the rules in sufficient detail and are subject to interpretation of the writer or presenter.

Step 1: Obtaining a Copy of the Rules

Once you've decided to begin, obtaining a copy of the rules is the first step. This may seem like a simple first step, but it, too, can be a daunting task. Regulations are officially published in the *Federal Register*. HIPAA's administrative simplification regulations may be downloaded from the Department of Health and Human Services (HHS) Web site (http://aspe.hhs.gov/admnsimp/Index.htm). Downloading an electronic version rather than acquiring a paper copy allows you to search the rule to find references more easily.

The Web site offers two versions for downloading: the text version or the Portable Document File (PDF) version. Each has advantages and disadvantages. The text version is easy to download for anyone using Microsoft Word. You can easily change the size of the font for easier reading, cut and paste directly from this version, and search the document using Word's Find feature. The text version, however, does not retain the same page numbers as the official *Federal Register* version and prints out as a longer document.

The PDF version requires you to download a free version of the Adobe Acrobat reader (if you do not already have this software). It is not quite as easy to manipulate as the text version, but it contains the official page numbers.

Another consideration in obtaining a copy of the rules is whether to download both proposed and final rules. Every rule begins as a proposed rule, with a period for public comment. The published final rule contains a summary of the comments. You may be tempted not to download the proposed rule when a final rule exists; however, the proposed rule may lend insights into why the final rule is written as it is, and this information may be helpful in implementing the final rule.

Step 2: Understanding the Rule Contents

After you have acquired a copy of a rule, recognize that only a small percentage of the pages are the actual rule. The remainder of the pages is the preamble, which describes the purpose of the rule, addresses the comments to the proposed rule, may review the standards selection process, and provides a governmental cost impact study. You may find the preamble useful-for example, its response to the comments provides justification for the final standards in the rule and even some assistance in interpretation-but, initially, you may want to begin by reading the rule itself. For the privacy rule, for example, the final rule can be found in the last 34 pages of the PDF version.

Step 3: Understanding the Terms

Each final rule contains definitions of terms used in the rule. These terms have very special meanings, so review them before reading the remainder of the rule. Key terms in HIPAA's proposed and final transactions, identifiers, security, and privacy rules include:

Covered entity: a health plan, clearinghouse, or provider (entity that furnishes or bills and is paid for healthcare services in the normal course of business) that transmits any health information in electronic form in connection with specified transactions. All of the rules provide specific examples of covered entities, and the final privacy rule describes several types of organizational relationships that should be understood as its requirements are implemented.

Business associate: in the final privacy rule, this term identifies a person or entity who performs any function involving use or disclosure of individually identifiable health information or who provides services to a covered entity that involves disclosure of individually identifiable health information.

The privacy rule requires a **business associate contract** to exist between the covered entity and business associate to protect health information.

The proposed security rule calls for a **chain of trust partner agreement** between two business partners in which the partners agree to electronically exchange information and protect the integrity and confidentiality of the data exchanged. The term "partner" has a very specific legal meaning and was changed in the final privacy rule to "business associate." This would suggest that the final security rule may also use similar language. However, government representatives have indicated that the concept of the chain of trust agreement is somewhat different than the business associate contract in the privacy rule.

The term **trading partner** is also used throughout the rules (especially in the transactions rule) to refer to an organization with whom a covered entity exchanges information. HIPAA does not explicitly require a **trading partner agreement**, but this agreement describes the specific communications protocols and other contractual issues relative to the exchange.

Permitted: action that is allowed, including that a covered entity may decide not to take that action.

Required: action that is mandated by the HIPAA law itself or the regulation.

Protected health information: individually identifiable health information that is transmitted by electronic media, maintained in any medium, or transmitted or maintained in any other form or medium.

Individually identifiable health information: information that is a subset of health information, including demographic information collected from an individual, and:

- is created or received by a provider, health plan, employer, or clearinghouse
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual

Work force: employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under its direct control, whether or not they are paid by the entity.

Treatment: the provision, coordination, or management of healthcare and related services by one or more providers, including the coordination or management of care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for care from one provider to another.

Payment: includes an extensive list of activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits. Payment also refers to the reimbursement for the provision of care, as well as other activities, including those associated with reviewing medical necessity, utilization review activities, and disclosures of specified information to consumer reporting agencies.

Operations: include a wide variety of administrative and financial activities to maintain the viability of an organization. Briefly, operations includes conducting quality assessment and improvement activities, creating de-identified health information, fund raising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in the privacy rule, as well as other activities.

Transaction: the transmission of information between two parties to carry out financial or administrative activities related to healthcare.

Step 4: Distinguishing Between Standards and Implementation Features

HIPAA's rules call for the adoption of industry-developed standards where they exist, or standards the government has created where industry-developed standards do not exist. Some of the standards are very specific, with formal implementation guides referenced; others are quite general, with only implementation features described.

The transactions rule calls for adoption of standards created by the designated standards maintenance organization (DSMO) ASC X12N. Implementation guides for these standards are published by the Washington Publishing Company (www.wpc-edi.com/). The guides spell out precisely the format and data content required for transmission of financial and administrative transactions data among covered entities.

The proposed security rule does not reference a specific DSMO-published standard, but rather provides a framework within which covered entities must adopt standards to meet their business needs. The proposed security rule references a number of standards developed by DSMOs, but none of these are explicitly required. Instead, the proposed rule includes security requirements and implementation features.

Although the final security rule is expected to be structured very similarly to the proposed rule, it is possible that subsequent modifications to the security rule may require adoption of specific DSMO-developed standards. In particular, we may expect to see in a year or so after publication of the final security rule a specific standard for electronic signature, such as a public key infrastructure (PKI) standard.

The final privacy rule is somewhat similar to the security rule in that it does not reference specific DSMO-developed standards. In the case of the privacy rule, however, the requirements and implementation features are more specific than in the proposed security rule.

Step 5: Interpreting the Rules

A final step in reading the rules is interpretation. The proposed security rule is intended to be flexible, scalable, and technology neutral. The privacy rule applies the legal principle that action is judged on the basis of what a reasonable person would do under the circumstance. Even the transactions rule provides options for providers so that those who want to continue using paper or do direct data entry instead of adopting the ASC X12N standards directly may do so.

Flexibility is good in the sense that it accommodates all covered entities, from solo practitioner offices to large integrated delivery networks or huge insurance businesses. On the other hand, flexibility means that the rules are subject to interpretation. This is why everyone needs to read the rules for themselves. Many organizations, vendors, consultants, and others may attempt to sway public opinion, increase sales of products, or generate business on the basis of misinterpretation. Even covered entities themselves may attribute more strict or more loose interpretation to suit their concerns.

Finally, the industry as a whole has often experienced regulators who appear not to follow a more flexible intent of a law when an investigation is conducted. This has left the industry skeptical about HIPAA and therefore vulnerable to those claiming solutions.

The most important thing a covered entity can do to ensure compliance is to read the rules thoroughly and carefully. Seek advice from those with a strong background of participation in the DSMOs or other organizations named in the law as advisory to HHS. Understand the rules and create solutions to meet specific business needs. Document your decisions. Then, as rules are implemented, you can continuously build a supportive environment and monitor for improvement.

Margret Amatayakul *is the founder and president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL. She can be reached at* margretcpr@aol.com.

Article citation:
Amatayakul, Margret. "Five Steps to Reading the HIPAA Rules (HIPAA on the Job series)." *Journal of AHIMA* 72, no.8 (2001): 16A-C.