Managing Information Privacy & Security in Healthcare

Health Insurance Portability & Accountability Act of 1996 (HIPAA)¹

By Barbara Demster, MS, RHIA, CHCQM

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the Department of Health and Human Services to issue regulations for medical privacy for providers, health plans and clearinghouses if Congress failed to pass a medical privacy act by August of 1999. Congress did not meet this deadline, and the Secretary published the Privacy Rule in December 2000 with the final modifications on August 14, 2002. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. The HIPAA Omnibus Rule, effective as of March 26, 2013 and with a compliance date of September 23, 2013, implements a number of provisions of the HITECH Act to strengthen the protections for health information established under HIPAA.

The major publications by the Secretary of the Department of Health and Human Services (DHHS) related to the Privacy Rule are listed below and may be accessed through the DHHS website at http://www.hhs.gov/ocr/privacy. The Preamble is very important to read as it provides examples, context, and insight into the Rule. This can be very helpful when applying the Privacy Rule to such a broad range of healthcare settings.

1. The Final Privacy Rule - December 28, 2000
   - Preamble: Federal Register Pages 82462 to 82798 (336 pages)
   - Final Rule: Federal Register Pages 82798 to 83829 (31 Pages)
2. Amendments to Part 160 - May 31, 2002
3. Amendments to Part 160 and 164 - August 14, 2002
4. Combined Unofficial Regulation Text
5. OCR Guidance Explaining Significant Aspects of the Privacy Rule - December 4, 2002
6. Omnibus HIPAA Rulemaking

The OCR Guidance is a very helpful document published originally in December of 2002 and updated since then by OCR. The OCR Guidance discusses in plain English major areas of the rule with a section on “How the Rule Works” followed by a section responding to “Frequently Asked Questions.” The document is very helpful and a must read not only to better understand the rule but also to understand the expectations of the enforcing agency.

The official HIPAA Privacy website of the Office for Civil Rights is http://www.hhs.gov/ocr/privacy/. Questions on the privacy rule may be submitted to OCRprivacy@hhs.gov.

Who is Covered Under HIPAA?
The article “Who’s Covered by HIPAA?” <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_009585.hcsp> summarizes the issues that define who must comply with the HIPAA regulations. While covered entities are covered by the HIPAA regulation (clearinghouses, health plans, and “certain” health care providers), the regulations are written in such a manner as to extend their reach to non-covered entities which fall within the ambit of “Business Associates.” A business associate is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A business associate also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

The Privacy Rule allows covered entities to disclose protected health information to the business associate if satisfactory assurances have been obtained that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity’s duties under the Privacy Rule. These satisfactory assurances generally take the form of a written business associate agreement between the covered entity or business associate and their respective business associates to ensure that these business associates will appropriately safeguard protected health information.

Coverage under HIPAA is also muddled by complex organizations that contain a mix of covered and non-covered entities. Individual covered entities may also coalesce to form either an Affiliated Covered Entity (ACE) or an Organized Health Care Arrangement (OHCA). The nature of the arrangements and agreements has an impact on how the rules are applied. This is discussed in the article “United Under HIPAA: A Comparison of Arrangements and Agreements (HIPAA on the Job)”<http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_014066.hcsp>.

A Covered Entity Decision Tool can be found on the CMS website <http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html>. If an organization has doubt about their covered status, they may answer a series of questions in this electronic tool to determine whether or not they are a Covered Entity.
Who is Excluded Under HIPAA?
Many institutions are not covered under HIPAA. For example, education records are covered under the Family Educational Rights and Privacy Act (FERPA) for schools that receive funds under an applicable US Department of Education program. In addition, employment records, even if the information in those records is health-related, are not covered by HIPAA.

What is the Scope of the Privacy and Security Rules?
The Privacy Rule governs permitted uses and disclosures of Protected Health Information (PHI) by covered entities and business associates. The Privacy Rule applies to PHI of all types (e.g., oral, written, recorded, and electronic). The Security Rule requires administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of PHI in electronic form.

Protected health information (PHI) means Individually identifiable health information that:

1. Is created or received by a health care provider, health plan, employer, health care clearinghouse, or prescription drug card sponsor;

AND

2. Relates to the past, present, or future physical or mental health or condition of an individual;

OR

3. Relates to the provision of health care to an individual;

OR

4. Relates to the past, present, or future payment for the provision of health care to an individual;

AND

5. Identifies the individual;

OR

6. There is a reasonable basis to believe the information can be used to identify the individual.

AND

7. Is transmitted by electronic media;

OR

8. Is maintained in any medium described in the definition of electronic media at § 162.103;

OR

9. Is transmitted or maintained in any other form or medium.

AND

10. Excludes individually identifiable health information:

a) In education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;

b) In records described at 20 U.S.C.1232g(a)(4)(B)(iv);

c) In employment records held by a covered entity in its role as employer; and

d) Regarding a person who has been deceased for more than 50 years.

While the HIPAA Administrative Simplification Statute was built around standardizing electronic transactions, the importance of covering all media forms was apparent during the development of the privacy regulations. As explained in the Privacy Rule’s Preamble, the response to the proposed rule overwhelmingly supported covering all media forms (oral, paper, electronic, etc.) with justifications
ranging from increasing patient confidence by total coverage to the administrative and fiscal burden of managing a complex system of fractured coverage.

The Security Rule, however, only applies to Protected Health Information (PHI) that is processed or transmitted electronically (ePHI). The Security Rule covers all ePHI of a covered entity wherever it is created, received, transmitted, or maintained. The Security Rule covers all ePHI of a business associate wherever it is created, received, maintained, or transmitted. The DHHS website has a link to the NIST HIPAA Security Rule Toolkit (http://scap.nist.gov/hipaa/) which is a self-assessment survey intended to help organizations better understand the requirements of the HIPAA Security Rule (HSR), implement those requirements, and assess those implementations in their operational environment.