



Managing Information Privacy & Security in Healthcare

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

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 major publications by the Secretary of the Department of Health and Human Services related to the Privacy Rule are listed below and may be accessed through the DHHS website at <http://www.hhs.gov/ocr/hipaa>. The actual privacy regulation text is relatively short (31 pages) when compared with the prefacing Preamble (336 pages) that discusses the rationale for each section of the final rule. The Preamble is very important to read as it provides examples, context, and insight into regulation. This can be very helpful when applying a 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

The combined "Unofficial" version is posted on the website of the Office for Civil Rights, the DHHS office responsible for enforcing the privacy regulations. This version of the regulation text contains not only the Final Privacy Rule with amendments integrated into the text, but also the Security Final Rule and General Administrative Requirements.

The OCR Guidance is a very helpful document published originally in December of 2002 and updated since then by OCR. The 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/hipaa/>. 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 there are three basic entities covered by the HIPAA regulation (clearinghouses, health plans, and “certain” providers) the regulations are written in such a manner as to extend their reach to non-covered entities in the form of Business Associates. Just because an organization does not fall into one of the three covered categories does not mean that it has no obligations under HIPAA if it does business with one of the covered entities. The obligations are spelled out in the required Business Associate agreement that must be made with Covered Entities.

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 <Link <http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp>>. 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

Generally speaking, HIPAA has a narrow focus on the entities that it covers. Other than the three entity types mentioned in the section above, the rest are excluded from coverage under HIPAA. The most notable exclusions are financial institutions, school records and employee records. Much of this is due to other privacy laws that cover these records. Education records are covered under the Family Educational Rights and Privacy Act (FERPA). Section 1170 of the HIPAA Statute (PL-104-191) passed by Congress in 1996 (as opposed to the regulations written many years later) specifically exempts financial institutions from HIPAA Administrative Simplification. The Right to Financial Privacy Act of 1978 (RFPA) and the Financial Services Modernization Act of 1999, most commonly called Gramm-Leach-Bliley Act or GLB, cover privacy of financial institution data.

Section 1170 of the HIPAA Statute reads:

“PROCESSING PAYMENT TRANSACTIONS BY FINANCIAL INSTITUTIONS

To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.”

What Information Is Covered

Information covered under the privacy rule differs from that covered under the Security Rule. To determine the information protected under the privacy rule, it is necessary to piece together the definitions of the terms used in that definition: health information, individually identifiable health information, and protected health information. This translates to the following definition of PHI:

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

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

OR

(2b) Relates to the provision of health care to an individual;

OR

(2c) Relates to the past, present, or future payment for the provision of health care to an individual;

AND

(3a) Identifies the individual;

OR

(3b) There is a reasonable basis to believe the information can be used to identify the individual.

AND

(4a) Is Transmitted by electronic media;

OR

(4b) Is Maintained in any medium described in the definition of electronic media at § 162.103;

OR

(4c) Is Transmitted or maintained in any other form or medium.

AND

(5) Excludes individually identifiable health information in:

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

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

c) Employment records held by a covered entity in its role as employer.

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 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 wherever it is received, generated, processed, stored, or transmitted by a covered entity. This becomes a moot point as the Privacy Rule in §164.530(c)(1) includes a safeguard standard requiring a covered entity to have in place appropriate administrative, technical and physical safeguards for PHI. The Security Rule is composed of nine administrative, four physical, and five technical safeguards focused on electronic data. When implementing security programs, organizations have implemented the [security rule](#) and include PHI in all its media forms (electronic, paper, fiche, oral, etc).