

The Privacy Rule

March 2003, Vol. 50, no.2

On April 24th of this year, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996, also known as HIPAA, take effect. Every physician's practice that bills electronically (a Covered Entity), whether directly or through a billing service, is covered by the Act and is expected to be in compliance by that date.

The Rule is complex, and it is likely that a relatively large number of practices will not be fully prepared to be in compliance with the mandates of the Rule by the compliance date. Failure to comply with the Rule may result in significant civil and criminal penalties. The Federal Government intends to begin inspections of physicians' practices on or after April 14th in order to determine compliance.

In brief, the Rule requires the following:

- Written notification of all patients about their privacy rights and the ways in which their health information will be used.
- Establishment and implementation of written privacy policies and procedures for each Covered Entity (practice).
- Training the practice's employees to ensure their understanding of the requirements of the Privacy Rule.
- Appointment of a Privacy Officer for the practice whose duty it is to ensure that the practice's privacy policies and procedures are established and carried out.
- Establishing security measures to ensure that patients' health information is available only to those individuals who need to have access to it.
- Creation of Business Associates contracts with individuals and firms who utilize Protected Health Information (PHI) of patients in fulfillment of their contractual duties.

It is important to note that the Privacy Rule supersedes State law unless State law is more stringent than the Rule.

HIPAA last modified the Rule in August of 2002. Some of these modifications are significant.

- Obtaining written consent from patients to use and disclose PHI for the purposes of treatment, payment, and business operations (TPO) was changed from mandatory to voluntary.
- Practices (Covered Entities) who provide direct patient care are now required to provide copies of the Notice of Privacy Practices to each patient, or to his / her Personal Representative not later than the first service occasion following April 14, 2003, in addition to the requirement of posting the Notice in a conspicuous location at the practice. The practice is required to obtain a written receipt signed by each patient that indicates that the patient received a copy of the Notice of Privacy Practices. This receipt should be retained in the patients' records at the practice.
- The authorization requirements have been modified to permit the use of a single authorization form for the disclosure of Protected Health Information (PHI) instead of the three separate forms originally required.

Clearly, the implementation of the Privacy Rule requirements will carry with it an increase in the non-medical workload of a practice. It is equally clear, however, that the Federal Government is serious about the Rule and will impose civil and criminal penalties for deliberate failure to meet the requirements. The Office for Civil Rights of the Department of Health and Human Services (HHS) has been authorized to ensure compliance and investigate complaints.

It is, therefore, important that each of us who is a Covered Entity become fully familiar with the mandates of HIPAA's Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule). Information may be obtained over the internet at the following addresses:

<http://www.medical-society.com>

<http://www.hhs.gov/ocr/hipaa>

<http://www.hipaaadvisory.com>

In addition, HIPAA information is available from the web sites of the various professional colleges as well. I hope the new regulations will be less intrusive than is generally anticipated.

Suresh C. Anand, M.D.

President