

# HIPAA Basics:

## An Overview Of HIPAA Privacy

by Bruce A. Smith

The recently issued final privacy regulations under 1996 Health Insurance Portability and Accountability Act (HIPAA) are, for now, the "next big thing" for physicians. The purpose of this article is to provide a very brief overview of those regulations.

### *Adoption of Privacy Regulations*

After Congress failed to meet its deadline to adopt health privacy legislation, the Department of Health and Human Services ("DHHS") published proposed privacy regulations in November 1999. Following an extended comment period during which DHHS received over 52,000 written comments, DHHS issued its final privacy regulations in December 2000 (the "Final Regulations").

### *Who is Covered?*

Three types of health care organizations ("Covered Entities"): health plans, health care clearinghouses (for example, billing companies) and certain health care providers. Providers – including physicians – are covered if they electronically store and transmit health care information, such as information on claims status, eligibility and referrals, or if they employ a third party to process their billings, and that third party stores transmits, and processes those claims electronically.

### *What Information is Covered?*

Protected health information ("PHI"), which is defined as information created or received by a health care organization or employer that relates to an individual's past, present, or future health condition, in all forms including oral, written, and electronic.

### *When Must I Comply?*

The compliance deadline is April 14, 2003.

### *What Do the Final Regulations Require?*

**Patients must consent to most disclosures.** A patient's consent is required in nearly all situations involving the disclosure of the patient's PHI. Physicians will be required to obtain patient consent before sharing PHI for treatment, payment and health care operations. Additionally, separate patient authorization must be obtained for non-routine disclosures.

**Patients must be given specific privacy rights.** Patients will have

significant new rights to understand and control how their health information is used. Among other rights, patients will have access to their medical records and the right to request that they be amended (although such requests may be denied). Patients also may request restrictions on disclosure to others of their PHI and alternative means of communicating PHI.

**Disclosures of PHI without consent are limited.** With few exceptions, a patient's health information may only be used for health purposes. PHI generally may not be used for purposes not related to health care – such as disclosures to employers to make personnel decisions, or to financial institutions – without explicit authorization from the patient. Additionally, disclosures of PHI will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes.

**Contracts with business associates must protect PHI.** A Covered Entity must assure that its "business associates" – which could include a billing company, consultant, attorney and most other third parties which may obtain medical information from the Covered Entity – also

*Continued*

# HIPAA Basics

protects such information. To meet this requirement, providers must enter into contracts with each of its business associates which include this obligation.

**Administrative changes will be required.** Although the Final Regulations mandate the adoption of certain privacy standards, Covered Entities are afforded flexibility in designing their own policies and procedures to meet those standards which take in account their size and financial resources. Covered Entities generally will have to adopt written privacy procedures addressing who has access to protected information, how it will be used within the entity and when the information may be disclosed. Additionally, Covered Entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

forms, policies and procedures to help make compliance with the Final Regulations less painful. Physicians should, however, familiarize themselves with the essential components of HIPAA and be prepared to begin the process of implementing the HIPAA privacy mandates to assure that the April 14, 2003 deadline is met.

*Bruce A. Smith is a health care attorney with the Syracuse-based law firm of Wood & Smith, P.C.*