

In compliance...

...with HIPAA rules

by the Division of Advocacy and Health Policy

The U.S. Department of Health and Human Services (HHS) published two final rules in the February 20 *Federal Register* that address standards required by the Health Information Portability and Accountability Act (HIPAA). The first rule contains revisions to the transaction and code set standards; the second establishes the long-awaited HIPAA security standards. This article summarizes the provisions that are pertinent to surgeons and their staffs.

Transaction/code set standards

HHS expects all parties to comply with the October 16 deadline for the transaction and code set standards. The following changes were made to the transaction and code set standards:

- HHS has retracted its designation of the National Drug Codes (NDC) as the recognized code set for reporting drugs and biologics for all covered entities but retail pharmacies. This reversal means that physicians will continue to use the Healthcare Common Procedure Coding System (HCPCS) codes to report drugs.
- The rule revision refines certain components of standard health care claims submitted by physicians and institutions. Covered entities are expected to test their systems using the data elements contained in the modified standard. Surgeons should check with vendors and payors with whom they exchange electronic data to determine when those businesses will begin testing with the modified health care claim standards.

Security standards

The HIPAA security standards become effective April 21, and practices must be in compliance with those rules by April 21, 2005. For the past year, this column has offered surgeons guidance in their efforts to comply with the HIPAA privacy standards. The publication of the security standard serves as a natural transition to looking at how practices secure the electronic information governed by the privacy standards.

Around the corner

May

- ACS-sponsored basic and advanced coding workshops for surgeons in Atlanta, GA, May 29-30. Visit the ACS coding workshop Web page at <http://www.facs.org/dept/hpa/workshops/cdwkshop.html> to register.
- ACS-sponsored practice management course for surgeons, May 31 in Atlanta, GA. Visit the ACS Web page at <http://www.facs.org/dept/hpa/workshops/pmworkshop.html> to register.

The privacy standard has given patients the right to know how their physicians use and disclose patient information. The security standards also require practices to implement safeguards to ensure that patient information cannot be accessed by anyone who does not have the right to receive it.

The implementation processes a practice has used to become compliant with the HIPAA privacy standard will be useful in understanding the government's expectations under the security standard. As surgeons have worked to ensure the privacy and confidentiality of patient information, their practices have already looked at some of the essential elements of security.

At this juncture, each practice should have assessed whether the physical location of computer terminals and fax machines adequately ensure that no unauthorized individuals have access to confidential information. A privacy officer should have set up access protocols for staff members (such as passwords, automated level-

continued on page 39

of president-elect of the Illinois State Medical Society (ISMS) during its recent annual meeting. Dr. Printen, associate professor of surgery at Northwestern University Medical School, is considered a pioneer in the area of bariatric surgery. He also is a practicing general surgeon based in Evanston, IL.

The Royal College of Surgeons of England recently awarded honorary fellowship to **Martin C. Robson, MD, FACS**, emeritus professor, department of surgery, University of South Florida, Tampa. Dr. Robson was

one of three physicians receiving the honor and the only one from outside the United Kingdom. He is a recognized expert in the field of wound healing and is currently involved in active clinical and basic science research on the subject at the Bay Pine Veterans Affairs Medical Center.

The Joint Commission on Accreditation of Healthcare Organizations named **Robert B. Smith III, MD, FACS**, to serve as its treasurer this year. Dr. Smith is the medical director at Emory University Hospital in

Atlanta, GA, and has served on the JCAHO's board since 1996. Additionally, he served on the College's Board of Governors from 1991 to 1997.

The College's New Jersey Chapter passed a resolution late last year recognizing **Kenneth B. Swan, MD, FACS**, for 20 years of dedicated effort to presenting and maintaining the Advanced Trauma Life Support course at the University of Medicine and Dentistry of New Jersey-New Jersey Medical School, Newark. Dr. Swan is a professor of surgery at the institution.


IN COMPLIANCE, from page 26

of-access controls on the computer system), ensuring that only the individuals who need to create or update patient records can do so. The practice is making sure that medical records maintained electronically are regularly backed up so that a power outage or a computer crash will not prevent necessary access to those records. All of these tasks are part of security compliance.

Just as the HIPAA privacy standard required practices to appoint a privacy officer, the security standard requires that a member of each physician's staff is designated as the officer for security activities. In a small practice, it is very likely that the same individual will serve in both capacities, while a larger practice might look to the staff member who is responsible for office and/or personnel management. The security officer's responsibilities will include working with both staff members and vendors.

Practices should conduct self-audits to examine current security practices. A beginning point for this could be the development of a diagram that tracks how patient information is handled from the time a new patient arrives to when that patient's records are purged or destroyed. Once

again, as with the privacy standards, the findings from the self-audits should be used to develop written policies and procedures to document how confidential information is handled. Practices also must conduct training sessions to ensure that their employees understand and abide by the business procedures for securing patient information.

The College has identified resources in the public domain that will help surgeons and their staffs comply with all the HIPAA standards. A number of regional public/private industry groups have developed compliance tools and sponsor both face-to-face seminars and Web-based courses. Additionally, most state governments have created HIPAA-specific Web sites that provide information and guidance on state-specific issues, such as state privacy laws. A directory with links to these Web sites is posted at <http://www.facs.org/>. 

ACS guidance on HIPAA issues is based on information contained in the "Small Practice Implementation Guide," version 2.0 (<http://www.wedi.org/snip/public/articles/200211012.0final.pdf>), © 2002, The Workgroup on Electronic Data Interchange.