

In compliance...

...with HIPAA rules

by the Division of Advocacy and Health Policy

As part of the health care industry's process to help small practices to comply with the privacy and security requirements in the Health Insurance Portability and Accountability Act (HIPAA), the WEDI Strategic National Implementation Process has created the "Small Practice Implementation Guide." Appendix A of that guide offers a simple model audit tool, which surgical practices may use to determine whether they need to make any changes.

True or false?

Some statements worth considering as you determine whether your practice is compliant with the mandates are as follows:

- My office does not use a patient sign-in sheet that includes confidential patient information, such as reason for visit, and so on. T/F
- My office does not place patient schedules in any places that may be seen by patients or other non-staff individuals. T/F
- In my office, all confidential conversations take place to the maximum extent possible in areas that cannot be overheard by other patients or non-staff individuals. T/F
- In my office, patients and non-staff individuals cannot gain access to our computers or fax machines and cannot view our computer screens. T/F
- Each computer user in my office has a personal computer password. These passwords change on a regular basis, and passwords of terminated employees are deleted immediately. T/F
- In my office patients and other non-staff individuals do not have any opportunities to access patient medical records, laboratory reports, and faxes. T/F
- My office has formal, documented procedures to ensure patient confidentiality when transferring to other offices paper files, orders, images, and specimens. T/F
- My office has formal documented procedures for accepting confidential patient information from outside of our office. T/F

- My office has confidentiality statements in place, and we inform patients of our confidentiality policies. T/F
 - My office has formal privacy and security procedures regarding access to confidential information, access to computer information, and access to areas of the office that may contain confidential information. T/F
 - My office requires the return of all keys and other items that allow access to the office and to computer files when a person no longer is authorized to access information. T/F
 - My office has formal privacy and security policies for all office personnel, and training for all office personnel is documented. T/F
 - My office uses laptops or other portable equipment (personal data assistants, electronic ordering systems, and so on) that hold confidential patient information, but this equipment is secure and can only be accessed by authorized personnel. T/F
 - My office has policies and procedures in place to ensure patient confidentiality by off-site contractors, such as billing, accounting, and transcription services. T/F
 - My office has a comprehensive survey of all our computer systems, including all software. T/F
 - My office has a disaster plan to protect patient information and contingency plans in the event of a computer systems failure. We also perform regular virus checks and correct any identified problems. T/F
 - All confidential information—paper and electronic—is stored with appropriate safeguards. T/F
 - Internet transmissions, including e-mail and telephone conversations, are secure. T/F
 - My office requires patients to sign a consent form. T/F
 - My office has confidentiality statements on all faxes and e-mail sent by the office staff. T/F
- If you find any of the statements are "false," you may need to change some office procedures. Main-

continued on page 44

Spring Meeting Web cast highlights key issues for the twenty-first century surgeon

An opportunity to visit "A Town Meeting—The Twenty-First Century Health Care System," which opened the College's Spring Meeting, April 14, in San Diego is now available through the College's Web site. A Web cast of this important session, the Assembly for General Surgeons, can be accessed by visiting the College's home page at <http://www.facs.org> and scrolling down the page. The following speakers' presentations are included in the Web cast:

- The Honorable David Satcher, MD, PhD, former Assistant Secretary for Health and U.S. Surgeon General: The U.S. Health Care System.

- Sir Barry Jackson, MBBS, MS, FRCS, FACS(Hon), president-elect of the Royal Medical Society: The National Health System: Directions and Lessons.

- Don E. Detmer, MD, FACS, Dennis Gillings Professor of Health Management, University of Cambridge: To Err Is Human: Will We Cross the Quality Chasm? The Institute of Medicine Perspective.

- Anthony A. Meyer, MD, FACS, professor of surgery, University of North Carolina: Quality Surveillance and Outcome Reporting.

- George F. Sheldon, MD, FACS, professor and chairman, department of surgery, Univer-

sity of North Carolina: Evolving Health Workforce Shortage—Failed Expectations?

- Haile T. Debas, MD, FACS, dean, school of medicine, University of California, San Francisco: Professionalism in Clinical Practice.

- A. Brent Eastman, MD, FACS, University of California, San Diego, and ACS Regent: Professionalism in Clinical Practice.

Visitors can download a high-speed or low-speed version of each speaker's presentation, and a text transcript accompanies each speaker's remarks.

IN COMPLIANCE, from page 32

taining the confidentiality of patient information and allowing appropriate access to that information within and outside of your practice is key to HIPAA privacy compliance.


This audit tool is a preliminary step and is not intended to be a comprehensive guide to meeting HIPAA privacy and security regulations. The industry is developing additional tools to help you and your staff to comply with these requirements. The College will bring those materials to your attention as they are introduced.

Proposed changes

On March 27, 2002, HHS issued a notice of proposed rulemaking making a series of proposed changes to the privacy rule. One of these changes rescinded the requirement that your practice develop authorization forms to receive a patient's consent for the use and disclosure of confidential patient information. You will still need to give a copy of the practice's "Notice of Privacy Practices" to your patients and document that the notice has

been given or that a good faith effort was made to provide the notice. To accomplish this, you may want to have patients sign a form acknowledging that they received the notice and place that form in the medical record. In future editions of "In compliance," we will review the documents your practice will need to develop.

Tip for privacy officer

HIPAA will require practices to develop a privacy policy manual where you keep all of the policies and forms you have developed to comply with the regulation. The practice staff members need to have access to the information in the manual. Are you going to maintain that document electronically or on paper? 

ACS guidance on HIPAA issues is based on information contained in the "Small Practice Implementation Guide" version 1.2 (<http://snip.wedi.org/public/articles/indexcfm?Cat=17>), © 2001, The Workgroup on Electronic Data Interchange.