

In compliance...

...with HIPAA rules

by the Division of Advocacy and Health Policy

This month's column picks up where we left off last month regarding materials that need to be included in a practice's privacy manual to ensure the confidentiality of patient information, especially when others may be able to access it. Following are some suggested items for inclusion.

- *Assurances from business associates to safeguard confidential information that your practice shares with them.* A business associate is defined as a person or organization that is not a member of your staff but performs a function that uses confidential information from your practice. A good example of a business associate might be a health care clearinghouse that submits the practice's claims. Plumbers, electricians, office equipment repair people, and mail carriers are not considered business associates. In most cases, companies that provide janitorial services are not considered business associates, unless the practice has contracted with them to handle or shred medical records. Practices will need written contracts or similar agreements with business associates that list the permitted and required uses and disclosures of confidential information. Practices may look at the sample contract language on the U.S. Department of Health and Human Services (HHS) Office of Civil Rights Web site listed in "Sample Business Associate Contract Provisions." (See "Tip for privacy officer" on page 35.)

- *Procedural and physical safeguards to protect and ensure the security of confidential information.* What are the practice's procedures for patients' and other visitors' access to the office beyond the waiting room? How are the records maintained and secured? What measures do you take to ensure the security of the confidential information when it is housed on your computer system or transmitted by modem or fax? If there is a fire, flood, or computer breakdown, what is your contingency plan to recover and secure the records? You will have to document the answers to these questions in writing and include the documentation in the privacy manual.

- *Access and audit control.* Each practice must establish and document levels of staff access to patient records. During this process it is important to ensure the staff understands what the practice considers to be unauthorized use, disclosure, modification, and destruction of confidential patient information. In electronic medical records systems, there must be a mechanism for identifying and tracking who has accessed or attempted to access confidential information. The privacy manual must specify who may access the log and how the log will be reviewed to identify potential weaknesses or actual breaches of security. Because of the required privacy provisions, there is good reason to believe that all electronic health systems will soon have auditing capability. At the present time, there is no comparable requirement for paper medical records.

- *Training.* All members of the staff must be trained to handle your practice's policies and procedures for handling confidential information. This training needs to be targeted to the appropriate level that allows them to perform their duties. Training could be done individually or in a staff meeting to discuss how the practice will handle privacy concerns or by having the staff review the practice's notice of privacy policies. During training, the practice's privacy officer should emphasize that the practice is open to staff observations of lapses in compliance with privacy procedures and that staff members should feel comfortable approaching the privacy officer about their observations.

- *What if confidential information is disclosed?* A practice is obligated to make a reasonable effort to mitigate any harm that might result from the use or disclosure of confidential information in violation of its policies and procedures. A practice also must impose sanctions against staff members or business associates who do not comply with policies and procedures. Practically, sanctions could mean, at a minimum, retraining on privacy policies and perhaps noting the violation in an

continued on page 35

Nominations for the Board of Regents sought

During the October 2002 meeting of the Board of Regents, an ad hoc committee on the structure, composition, and terms of the Board of Regents made recommendations to the Board. One of the recommendations was the addition of new seats on the Board so that all specialties having Advisory Councils will have representation. The Board approved this recommendation and added three new seats.

The 2003 Nominating Committee of the Board of Governors has the task of selecting nominees for five seats on the Board of Regents that will need to be filled during the 2003 Clinical Congress. The following suggested guidelines are used by the Nominating Committee when reviewing the names of potential nominees

for election to the Board of Regents.

- Loyal members of the College who have demonstrated outstanding integrity and medical statesmanship along with an unquestioned devotion to the highest principles of surgical practice.

- Demonstrated leadership qualities that might be reflected by service and active participation on ACS committees or in other components of the College.

- Recognition of the importance of their representing all who practice surgery.

- Also to be taken into consideration are geography, surgical specialty balance, and academic or community practice.

- The College encourages consideration of women and other underrepresented minorities.

- Individuals who are no longer in active, surgical practice should not be nominated for election or reelection to the Board of Regents.

The surgical specialties that should be given priority consideration are:

- Colorectal
- General
- Neurological
- Orthopaedic
- Pediatric
- Vascular

Nominations should include a paragraph or two on the potential contributions each candidate can offer in terms of what he or she can do for the members of the College. Please submit nominations to memberservices@facs.org. The deadline for submitting nominations is March 17, 2003.


IN COMPLIANCE, from page 19

employee's record. Depending on how serious or flagrant the disclosure was, it could even lead to the dismissal of a staff member or the cancellation of a contract with a business associate.

When developing, organizing, and refining the practice's policy manual, remember that the contents of the manual must include procedures to address each item listed in the "Notice of Privacy Practices."

Tip for privacy officer

There is another resource for HIPAA privacy guidance. The Secretary of the HHS has assigned oversight of HIPAA privacy compliance to the Of-

fice of Civil Rights (OCR). A practice may want to bookmark OCR's Web site (<http://www.hhs.gov/ocr/hipaa/assist.html>) to review or download the document "Frequently Asked Questions About the HIPAA Privacy Rule." This document will be updated as OCR responds to questions posted on its Web site or develops additional guidance on privacy issues. 

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.Ofinal.pdf>), © 2002, The Workgroup on Electronic Data Interchange.