

In compliance...

...with the security rule under HIPAA

by the Division of Advocacy and Health Policy

On April 20, the security standards under the Health Insurance Portability and Accountability Act (HIPAA) will go into effect. So now is a good time to review how this rule and the privacy rule work together and to examine what surgical practices need to do to comply with the rules.

Privacy and security rules

The privacy rule under HIPAA, which became effective in its present form April 14, 2003, applies to all protected health information (PHI) for patients, whether it is in oral, written, or electronic form. The rule restricts the availability of that information to only those individuals who need to know the content of the records and reduces the inadvertent release of information.

On the other hand, the security rule applies only to those records that contain electronic protected health information (EPHI). EPHI is information that is created, received, maintained, or stored on a computer or any storage device that is hooked up to a computer (such as a magnetic disk, flash drive, or compact disc) or that is transmitted via the Internet. The purpose of the security rule is to protect the integrity of the electronic record.

While it is possible to imagine a physician's practice that is subject only to the privacy rule, as a practical matter, virtually all practices are subject to both rules. Both the privacy and security rules contain administrative, physical, and technical safeguards that the practice must meet, and the rules have been structured so that, wherever possible, a practice that meets the privacy standards will already be well along in compliance with the security rules.

Similarities and differences

Both rules require the practice to have written policies regarding a range of activities. In fact, the privacy rule is much more comprehensive, touching everyone in a practice. On the other hand, the security rule affects only indi-

viduals responsible for electronic systems, either working on a computer in the practice or overseeing related work done under contract to the practice.

Both rules also require the practice to have written policies covering a range of items, and both are very flexible in terms of exactly what will satisfy a requirement. However, the two rules differ with respect to what practices must document to satisfy the two rules.

The security rule is built around 18 standards that are general statements of security needs. Each security standard is then followed by implementation specifications designated as either "required" or "addressable." Required specifications must be implemented and documented in the practice's policies. Addressable specifications must be assessed in terms of whether they are reasonable and appropriate safeguards in the practice's environment; if the conclusion is that they are not, the practice must consider whether other safeguards could be substituted. For addressable specifications, the documentation in the final policy must outline the entire process of considering the original implementation specification and, if that is rejected, of considering any substitute actions.

Example of the two rules working together

The privacy rule requires that the practice "have and apply appropriate sanctions" against those who violate its privacy policies and procedures (45 C.F.R. § 164.530 (e)). The security rule requires that the practice "apply appropriate sanctions against those who fail to comply" with their security policies and procedures (45 C.F.R. § 164.308 (a)(1)).

The privacy rule simply says a practice must have policies to prevent disclosures of information in violation of the regulation. While the rule makes it clear which disclosures are permitted or prohibited, the practice must decide exactly which policies it will have. A practice simply documents its policies and does not have to document the rationale for the final policy.

Reassessment of policies

Both the privacy and security rules require that practices periodically reassess their policies. Because of the way these two rules fit together, it is probably best to review policies under the two rules together. In addition to annual or other periodic reassessments of policies, the need for further review may be triggered by certain events, such as a change in the data system or a change in the workflow in the office. Reassessment could be needed for less obvious reasons as well, such as if new furniture for staff results in a rearrangement of workstations, perhaps necessitating a number of changes in privacy procedures.

Organizational approaches

Each rule requires the practice to designate a person to be responsible for the development of policies and procedures under the respective regulation. Of course, the practice manager will bear the ultimate responsibility for the devel-

opment of policies under both rules. However, it is possible to split the responsibility for developing the policies among people. For example, a practice may find it useful to give responsibility for the portions of both the privacy and security rule that relate to systems to one person and responsibility for the remainder of the privacy rule to another person. This method has the advantage of assigning very technical “bits and bytes” work to a specialist in the field. If responsibility for developing the policies for the rules is split, however, the people responsible for developing the policies will need to work closely, and the policies will have to be integrated after they are completed. □

Addressable implementation specifications

In the security rule, an addressable implementation specification does not mean it is automatically optional. The practice must consider whether the specification is reasonable and appropriate given the environment and, if not, whether other safeguards could be substituted. Cost is certainly a factor that should be included in the analysis. The rationale for the final decision must be documented in the final security policy.