Another HIPAA deadline is looming—April 21, 2005, is the date for compliance with the Security Rule. By then, your ambulatory surgery center (ASC) must have plans in place to protect patients’ electronic protected health information (ePHI), as required by the Health Insurance Portability and Accountability Act.

A key difference from the more familiar Privacy Rule—the Security Rule applies only to electronic information. The Privacy Rule, already in effect, applies to all information, electronic, written, and oral. There is some overlap, so you may already be doing some of what the Security Rule requires.

Don’t put off your compliance effort, cautions Robert Tennant, senior policy advisor in health informatics for the Medical Group Management Association (MGMA). “Just like the privacy rule, it gets tougher if you leave it to the last minute. Read some of the materials that are available free and get up to speed,” he suggests. Then see if some areas require more effort than others. You may decide to bring in someone to assist with the more technical matters.

“If you wait, you are going to be scrambling.”

Focus on business processes

Instead of focusing just on what you need to do to comply with the rule, focus on security to protect your own business processes, Tennant suggests. For example, one rule requirement is a risk analysis of threats to your electronic information. Ask yourself, what could happen to your business if there were a breach in electronic security? What if your billing system crashed, and you lost a month of receipts? Do you have backups of patient records in case your system goes down?

“Basically, this is what a risk analysis is—walking through your facility and looking at the potential problems,” he says. These are areas you most likely will want to address anyway.

Some good news—the rule provides flexibility for small organizations like ASCs. The rule has both:

- Required elements, which must be implemented
- Addressable elements, which are required but allow flexibility. If these are not implemented, the facility needs to document why.

“The government says you can consider things like the size, complexity, and capability of your technical infrastructure, as well as the cost of implementing some of these measures,” Tennant says.

You also can consider the probability of a risk. There might be a small risk of a hacker getting into your system but a greater risk of a system failure for some other reason. You can rate the risks as high, medium, or low to set priorities.

Penalties under the Security Rule are not as onerous as for the Privacy Rule. Civil penalties are $100 per violation, up to $25,000 per year for each requirement violated. In contrast, Privacy Rule penalties can go much higher, up to $250,000 and / or 10 years in prison.

Because ASC managers typically aren’t computer experts, there may be a temptation to lean heavily on software vendors for compliance. But compliance is the ASC’s responsibility.

“If your vendor gives you a written statement that says, ‘We are HIPAA compliant,’ it is your responsibility to be sure they are doing what they need to do,” advises Barbara Harmer, RN, MHA, president of MedAssist Consultants, Celebration, Fla, who speaks frequently on HIPAA.

Do a gap analysis

A number of policies and procedures are required. ASCs should do a “gap analysis” by comparing existing policies and procedures with the rule’s require-
ments and develop new policies as needed. After the policies and procedures are finalized, employees and other workers need to be trained on the requirements. Training is required not only for employees but also for others who work in the facility such as contracted anesthesia providers, temporary personnel, and volunteers.

The rule has requirements for safeguards in three areas:

- administrative
- physical
- technical.

Here are some questions to ask for each area. These are examples only. For detailed information, see the resources at the end of the article.

**Administrative safeguards**

- Have you done a risk analysis and developed a risk management plan for ePHI? This is a key requirement of the rule.
- Have you assigned responsibility to a security officer? This might be your administrator or business manager.
- Do you have a workforce security plan? For example, do you have ways to ensure only appropriate employees have access to patient records? Do you have a plan for terminated employees, such as changing their passwords and retrieving their keys?
- Do you have sanctions for members of your workforce who fail to comply with security policies and procedures?
- Do you have a way of auditing use of confidential information?
- Have you done or are you planning to do security awareness and training for your staff?
- Do you have a procedure for handling security breaches?
- Do you have contingency plans for backing up and recovering your data and managing data in an emergency?
- Do you have business associate agreements with third parties who handle your ePHI? If you already have privacy agreements, these may have to be updated for security.

---

**Physical safeguards**
- Do you have a way of locking rooms where computers are located and electronic records are stored?
- Do you have a contingency plan for recovering data in case of a disaster or emergency?
- Do you have a way to keep unauthorized people from having access to ePHI?
- Do you have policies for security and proper use of workstations, including desktops, laptops, and personal digital assistants (PDAs) that belong to your facility?
- Do you have proper methods for disposing of electronic media, such as CDs, diskettes, and old computers?

**Technical safeguards**
- Have you assigned each authorized person a user name and password?
- Does your information system have an automatic logoff in case a person forgets to log off after a session? That prevents someone else from accessing the system without authorization.
- Have you considered using encryption when sending ePHI, such as prescriptions, over the Internet or other open system? Encryption is an “addressable” element of the regulation, meaning flexibility is allowed.
- Do you have a way of auditing that your information system is used appropriately?

**Help in complying**

There is no single checklist for complying with the Security Rule because it has several sections, Tennant notes. Off-the-shelf programs can help with compliance, though some are quite costly. There also are resources available for little or no cost. Resources geared particularly to small health care organizations are:
- WEDI/SNIP, a nonprofit workgroup that specializes in HIPAA implementation, offers free white papers at www.wedi.org/snip/. Look under What’s New.
- National Institute of Standards and Technology (NIST) has a new draft Introductory Resource Guide for Implementing the HIPAA Security Rule (Special Publication 800-66) at www.csrc.nist.gov. Look under Publications and scroll down to Drafts. The guide has examples for small and large organizations.
- HIPAA Toolbox from the Medical Group Management Association at www.mgma.com. Look under Store and search for HIPAA Toolbox. Price is $140 for MGMA members and $219 for nonmembers.
- Vendor template for meeting HIPAA security requirements. A checklist on what to ask vendors from the North Carolina Healthcare Information and Communications Alliance. Free at www.nchica.org/HIPAAResources/Samples ❖

*The final Security Rule was published in the February 20, 2003, Federal Register and is at www.cms.hhs.gov/hipaa/hipaa2/ regulations/security*
**HIPAA Security Rule**

**Basic requirements**
The security rule requires organizations to safeguard the integrity, confidentiality, and availability of patients’ ePHI during its:
- receipt
- creation
- storage
- transmission.

**Safeguards**
Safeguards are required in three areas:
- administrative
- physical
- technical.

**Key concepts**
The rule has:
- required elements: Must be implemented
- addressable elements: Flexibility is allowed, but if elements are not implemented, facilities must document why.

**What is not covered**
The Security Rule does not cover:
- paper-to-paper fax
- phone calls
- video conferencing
- voice mail messages.

**What is covered**
- computer-generated faxes
- fax-back services.