# Final Security Regulations Present Challenges, Opportunities for HIM



*by Dan Rode, MBA, FHFMA*

With the release of the final HIPAA security regulations in February, HIM has taken yet another step toward the transition from paper to the electronic health record (EHR). This article discusses key areas of security compliance and how your organization can be prepared.

## When PHI Goes Electronic

Electronic protected health information (PHI), essentially defined as PHI in an electronic medium or transaction, becomes the key focus under the security rule. An organization's efforts to meet the requirements for PHI are the basis for the protection of electronic versions of PHI.

The rule underscores the HIM professional's role in moving the industry to the EHR by establishing standards by which organizations must address administrative, technical, and physical aspects of electronic PHI. It reinforces the idea that electronic PHI security is an administrative activity, not an information technology activity. It recognizes, however, that information technology will be part of the resources used to meet the obligations HIPAA creates for the organization.

The rule also requires that an organization not only address the confidentiality of electronic PHI but also take steps to assess risks and protect the availability and integrity of health records through the implementation of risk assessment, policies, procedures, and training. The industry's concurrent moves toward the EHR and a national health information infrastructure will make these activities even more critical.

## Taking the Lead

HIM professionals have the challenge and the opportunity to take the lead not only in implementing the EHR, but also in ensuring ongoing confidentiality and security of the EHR and electronic PHI.
The rule also gives guidance in the latter process
that is useful today, even though the deadline for compliance is 2005.

For example, the rule says an organization must:

- ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the privacy rule
- ensure compliance by the organization's work force

There are 18 standards, and each has implementation specifications that are required or could be
addressed. Like the privacy rule, the security rule provides for a flexible approach. The standards take into account that no two covered entities are alike, nor are they on the same timetable for EHR implementation. But all entities must understand, address, and respond to the issues appropriately based on their environment, situation, and resources.

## Dealing with Designated Record Sets

As the profession addressed the privacy rule and PHI, we had to take into account an organization's "designated record sets" that contain PHI. One of the challenges of privacy rule implementation is that paper and electronic records are often used all

over an organization. For example, there may be electronic PHI in diagnostic areas, electronic claims in patient accounting or billing, and paper records as well. Conversion to the EHR will be paralleled by conversions in other systems within an organization. Organizations will need to address not only what goes out of the EHR but where incoming information comes from and where it is going.

The security rule calls for "administrative safeguards," and the Department of Health and Human Services (HHS) indicates that covered entities must implement policies and procedures to prevent, detect, contain, and correct security violations. This involves an organization's risk analysis, risk management, sanctions, and information system review activities. HHS not only suggests that these should be among the first steps of the organization's security rule implementation, but also suggests that this be an ongoing process, especially as the industry becomes more electronically based.

The rule also calls for a security official who is responsible for development and implementation of the policies and procedures required by the security rule. This individual ideally should be the organization's privacy officer—a perfect role for an HIM professional.

## Training: A Familiar Refrain

The rule's call for work force security training also resembles the requirements established for privacy. It includes initial and ongoing training of the entire work force, including senior management, as well as sanctions for those who do not abide by policies and procedures related to the rule. Covered entities are to include security reminders as part of their compliance processes.

Like the privacy rule's concept of "minimum necessary," the security rule addresses information access as a standard. While the implementation specifications are addressable, meaning the covered entity must assess whether the standard is reasonable and appropriate for the entity and would contribute to the protection of elctronic PHI, this section directly affects anyone with access to electronic PHI. In addition to the limitations surrounding access, the security rule also requires the monitoring of log-ins and password management, along with some response to security incidents.

The security rule also addresses the security of data from the perspective of having it available when it is needed and ensuring data integrity—clear requirements of any record system. The rule provides a contingency plan requirement and calls for three plans:

- a data back-up plan
- a disaster recovery plan
- an emergency mode operation plan

These requirements should be part of every organization's disaster plan, whether records are paper or electronic.

## Technical Expertise Is Key

In the electronic environment, many of these activities will call for technical options. Organizations will need to have the technical knowledge internally, use the technical knowledge available within the organization (usually a function of the information technology department), or purchase the knowledge elsewhere. At a minimum, HIM professionals must have basic information system knowledge in order to request support or determine options for resource consulting or purchase. This same knowledge is also needed for EHR implementation.

The security rule also calls for a number of "technical safeguards." The extent to which an organization will have to address these requirements is directly proportional to the degree of electronic systems and data it possesses. User IDs, emergency access procedures, automatic log-off, encryption and decryption, audit controls, integrity, electronic authentication, and transmission security should be addressed. The more "electronic" an organization is, the better the chance that technology expertise and resources are already available to the implementation team.

## Physical Security in a PDA World

There are also requirements covering physical security and organizational items such as adding language to business associate agreements to cover security. Physical security covers looking at contingency operations, security plans for physical access, tampering, and theft, access controls, including "visitors" (including the potential for patient access to EHR), and maintenance of records. Workstation security is key—not only for desktop computers and central systems but laptops and PDAs as well.

The surge in the use of laptops and PDAs containing electronic PHI will be a challenge for a variety of healthcare entities, especially those that provide care in patients' homes or outside the organization. This will call for technical security to prevent inappropriate access and medical record policies regarding information outside the traditional system or record.

## What Comes First?

First, it is important to thoroughly read the security rule. AHIMA has also provided an analysis on the rule available online at www.ahima.org/dc. More materials will be forthcoming.

Next, any purchase of information systems or technology now needs to be considered with the final security rule in mind. Organizations should not make or plan for a purchase without including pertinent information that covers the rule in a request for proposal. Any purchase should be made with compliant security components or with an agreement that the purchase will be upgraded to include all components needed to meet the security rule's provisions. Because most organizations take some time to make these purchases, it is not too early to begin your security process. This would be especially important for organizations in the process of purchasing EHR systems.

Remember, the April 21, 2005, implementation date is an "implementation by" date; there is no penalty for implementing early. (The compliance date does not apply to small health plans as defined in the HIPAA regulations.) Given that the security rule is also a good business rule, implementing early will be to the advantage of your organization.

Like any challenge, meeting the rule's requirements will take time and effort. But HIM professionals, many already on the road to the EHR, have the experience and education to promptly get on the path to compliance.

## Five Principles for Protecting Information

In March, AHIMA presented an audio seminar on the security rule's impact on privacy and HIM. Speaker Bill Braithwaite, MD, PhD, a principal author of the HIPAA regulations, mentioned five "principles of fair information practices" that the HIPAA privacy and security rules follow—principles very close to tenets followed by AHIMA. These include:

- Notice: existence and purpose of a record-keeping system must be known to the individual whose information is the subject of the record, thus the notice of privacy practices required under the HIPAA privacy regulation
- Choice: information is collected only with knowledge and permission of the subject and used only in ways relevant to the purpose for which the data was collected and disclosed only with permission or overriding legal authority
- Access: the individual, the subject of the record, has the right to see the record and ensure quality of information, meaning also the requirement that the record holder maintains accurate, complete, and timely information
- Security: that reasonable safeguards for confidentiality, integrity, and availability of information are in place
- Enforcement: that violations of an organization's privacy and security standards or policies result in reasonable mitigation and penalties

***Dan Rode*** *(dan.rode@ahima.org) is AHIMA's vice president of policy and government relations.*

---

**Article citation**:
Rode, Dan. "Final Security Regulations Present Challenges, Opportunities for HIM." *Journal*

*of AHIMA* 74, no.5 (May 2003): 14ff.