

CLEARING THE FINAL HIPAA HURDLE: PREPARING FOR COMPLIANCE WITH THE HIPAA SECURITY RULE

(AS PUBLISHED IN THE JULY/AUGUST 2003 ISSUE OF MICHIGAN HEALTH AND HOSPITALS)

ANDREW B. WACHLER, ESQ. AND AMY K. FEHN, ESQ.

On February 20, 2003, while most health care providers were in the midst of last minute preparations to become compliant with the HIPAA Privacy Rule, the Department of Health and Human Services (DHHS) published the Final HIPAA Security Rule.

The Security Rule applies to the same “covered entities” that are covered by the Privacy Rule and the Electronic Standard Transactions Rule and provides additional safeguards for “protected health information” that is maintained in or transmitted by electronic media.

The core structure of the Security Rule consists of eighteen standards, which are broken down into three basic categories: administrative safeguards, physical safeguards, and technical safeguards.

The administrative safeguard standards require covered entities to analyze the risks of unauthorized disclosure of electronic protected health information within the organization, implement a number of required policies and procedures and maintain certain documentation to manage and minimize risk.

Physical safeguard standards deal with the security measures taken to protect buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The policies and procedures required under this standard include policies to protect the physical locations that house electronic equipment, as well as the equipment itself.

Technical safeguard standards deal with the technological measures to safeguard and control access to electronic information, as well as the development and implementation of policies and procedures dealing with the use of technology.

Each standard also has certain “implementation specifications” that serve as the “instructions” for compliance. In an effort to make the final Security Rule more scalable and flexible, the implementation specifications are further broken down into those that are “required” and those that are “addressable.”

If an implementation specification is required, the organization must implement the specification as set forth in the Rule. For those specifications that are “addressable”, the organization may implement an alternative specification instead of, or in combination with, the specification set forth in the Rule. If an alternative approach is taken, the organization must document its decision not to implement the Security Rule’s specification, the rationale behind the decision, and the alternative approach that it has chosen.

In determining which specific technologies and security measures must be taken in order to meet the standards, an organization is permitted to take the following into account:

1. Its size, complexity, and capabilities;
2. Its technical infrastructure, hardware, software, and existing security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to electronic protected health information.

In some situations, the covered entity may also decide that the implementation specification is inapplicable to its situation and that the standard may be met without the specification or an alternative. In these situations, the covered entity must document its decision not to implement the specification, the rationale behind that decision, and the manner in which the standard is being met.

Although provider organizations have nearly two years remaining in order to meet the Security Rule's compliance deadline of April 21, 2005, organizations should develop a plan of action immediately. One reason for immediate attention is that the Privacy Rule, because of overlapping provisions, may already mandate many of the Security Rule requirements.

The Privacy Rule requires covered entities to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." Because the Security Rule is also broken down into administrative, physical and technical safeguards, and provides more specific guidance regarding the government's expectations, its requirements could potentially be taken into consideration by the government when determining what is appropriate or reasonable during investigation of an alleged Privacy Rule violation.

Another reason that organizations should begin taking immediate action is to provide adequate time for implementation of new technological and administrative systems. As many organizations learned during implementation of the Privacy Rule, this type of change cannot be expected to occur overnight.

The Security Rule requires organizations to designate a Security Officer who will be responsible for development and implementation of the required security policies and procedures. It is important to designate this person as soon as possible since this individual will be a key individual in the development of a HIPAA Security compliance plan. It is important that this individual develop a thorough understanding of the Security Rule's requirements. While it is important that the Security Officer have some understanding of technology, he or she will also need an understanding of the organizational structure and will need direct lines of communication with key management personnel in order to develop and implement the required administrative policies.

Although the Security Rule does not require a task force, it may be necessary from a practical standpoint in a larger organization. As discussed above, the Security Rule involves much more than the evaluation of software or hardware systems. In order to implement the requirements of the Security Rule in the most efficient manner, an interdisciplinary approach should be taken. For example, individuals from the IT Department will be able to discuss current technological capabilities, but may not be in the best position to address the personnel, policy and training issues associated with the use of technology.

It may also be helpful to include representatives from departments who perform day-to-day functions that are impacted by security measures. The “hands on” employees or their immediate supervisors are in the best position to discuss the current uses of electronic media within their respective departments, the levels of access needed by various categories of employees, and the practicality of certain suggested security measures.

It is also advisable to have legal counsel participate on the task force. As discussed above, the Security Rule requires organizations to analyze risks and to make judgment calls when determining which specific technologies and procedures to implement. Attorneys are accustomed to analyzing risks in addressing other compliance issues and should play a vital role in the risk analysis/risk management process required by the Security Rule.

The task force meetings should initially focus on the identification of all uses of electronic media within the organization and the associated risks. The task force should then focus on the Security Standards Matrix appended to the final Security Rule. This matrix sets forth each of the standards and implementation specifications and should be used as a “checklist” for compliance. The task force should consider each required specification and determine the steps that the organization will take in order to comply with the requirement. With respect to “addressable” specifications, the task force should discuss and determine (1) whether the specification is applicable to the organization; (2) if applicable, the feasibility of implementing the specification; and (3) if it is not feasible, alternative approaches that could be taken and the relative risks associated with each alternative.

A final copy of the Security Rule, as well as additional information, can be accessed at the CMS Administrative Simplification website: <http://www.cms.hhs.gov/hipaa/hipaa2/>. The Security Officer of the organization should check this website on a regular basis for further guidance regarding implementation of the Security Rule.