AHA
Advancing Health in America

HOSPITAL HIGHLIGHTS

Prepared for AHA members whenever there is important HIPAA-related news.

CMS ISSUES LONG-AWAITED HIPAA SECURITY RULE

February 27, 2003

On February 20, the Centers for Medicare & Medicaid Services (CMS) published in the *Federal Register* the final security regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Hospitals and health systems have been waiting for more than two years for the final rule to be released. During that time, the AHA has continuingly urged the Department of Health and Human Services (HHS) to publish the final security rule because the security rule is inextricably linked to the HIPAA medical privacy rule. With less than two months left until the April 14 privacy compliance deadline, failure to expedite the release of the final security rule means hospitals face the needless added cost that will be incurred implementing the "reasonable safeguards" required by the privacy rule and almost immediately need to modify these safeguards to comply with the security rule. For example, the security rule requires hospitals to: (1) conduct a complete risk analysis; (2) document their assessment of the reasonableness of certain implementation specifications for their facility; (3) develop security policies and procedures; (4) revise their business associate agreements to incorporate additional security provisions; (5) remedy system deficiencies; and (6) train all of their workforce on their security procedures.

The AHA is pleased that the security rule simplifies or eliminates several administrative requirements that were duplicative or confusing in light of the privacy rule and that the privacy and security rules are now more compatible. However, we are disappointed that the long delay in issuing the final security rule unnecessarily strains hospitals' scarce resources.

The security rule becomes effective April 20, and hospitals have two years from the effective date – until April 20, 2005 – to comply. The security rule provides requirements in the following five categories:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation.

Because the final privacy rule also requires administrative, technical and physical safeguards to protect the confidentiality of protected health information, hospitals may wish to use the security rule's standards in thinking through the safeguards they are implementing for purposes of the privacy rule, especially with respect to protected health information that is maintained or transmitted using electronic media. CMS states that it intends to issue guidance and clarification of the security rule generally through written documents and postings on its Web site.

To view the final rule, go to www.access.gpo.gov/su_docs/fedreg/a030220c.html under HHS.

We have highlighted below some significant aspects of the security rule for hospitals.

Covers Only Electronic Protected Health Information
Although CMS states that security standards for "all health information or protected health information in nonelectronic form may be proposed at a later date," the final security rule applies only to electronic protected health information in storage and transmission. This means that each of the three sets of final HIPAA regulations is applicable to an entirely different subset of patient information: Privacy applies to virtually all protected health information maintained by hospitals; Transactions and Code Sets applies only to certain identified electronic transactions; and Security applies to protected health information that is stored or transmitted electronically, whether or not it involves one of the standard transactions. For example, electronic medical record systems and order entry systems will be subject to the security standards and CMS states that fax-back and voice response systems will generally require security measures by one of the parties involved. Information in oral, paper or other non-electronic format, however, is not covered by the security rule. Moreover, the preamble to the security rule makes clear that paper-to-paper faxes, person-to-person telephone calls, video teleconferencing, and voice-mail messages, where information is in non-electronic form before transmission, are not subject to the security rule. CMS also clarifies that copy machines, fax machines and telephones, even if they contain memory and can produce multiple copies, are not considered electronic media subject to the security rule.

Flexibility in Implementation
The security rule sets forth "general rules" which require that covered entities: "(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information . . .; (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) Protect against any reasonably anticipated uses or disclosures that are not permitted or required under [the privacy rule and]; (4) Ensure compliance with [the security rule] by its workforce."

Although these rules appear to set an incredibly high standard of security, in the preamble to the security rule, CMS recognizes that "there is no such thing as a totally secure system that carries no risks to security" and that ensuring protection does not mean "providing protection, no matter how expensive." In addition, we note that the security rule appears to provide for flexibility and scalability, as in the privacy rule. Specifically, covered entities, including hospitals, are permitted to "use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications" of the security rule. The security rule specifically allows hospitals to take into account the following factors in deciding what measures are reasonable and appropriate:

- the hospital's size, complexity and capability;
- technical infrastructure, hardware and software capabilities of the hospital;
- costs of security measures; and
- the "probability and criticality of potential risks to electronic protected health information."

Required and "Addressable" Implementation Specifications
The security rule provides additional flexibility with regard to its implementation specifications. The security rule sets forth standards (with which all covered entities must comply), and implementation specifications for those standards. Some of the implementation specifications are "required" and others are marked "addressable." For addressable implementation specifications, a

covered entity must assess whether the safeguard is reasonable and appropriate in its environment, in light of the potential security benefit to the entity's electronic protected health information. If the safeguard is determined to be reasonable and appropriate, the covered entity must implement the specification. If the covered entity determines that the safeguard is not reasonable and appropriate, the entity must document its reasoning and "[i]mplement an equivalent alternative measure if reasonable and appropriate." If the covered entity determines and documents that neither the particular implementation specification nor an alternative to that specification is reasonable and appropriate, the covered entity must take steps to ensure that it is nevertheless compliant with the standard set forth in the rule. The AHA finds this last requirement confusing and will ask CMS to clarify.

Security Risk Assessment
The security rule requires all covered entities to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." All covered entities must then implement security measures to reduce the risks and vulnerabilities identified to "a reasonable and appropriate level." This is similar to a gap analysis that many hospitals conducted with regard to implementing of the privacy rule; however, this assessment will identify potential security risks and vulnerabilities in electronic information systems rather than a gap in compliance.

Compatibility with Privacy Rule
As noted above, the AHA is pleased that the final security rule is much more compatible with the final privacy rule. For example, the security rule moves (but does not materially change) many of the definitions from the privacy rule to make them applicable to the requirements of both rules. In addition, the security rule incorporates the structural options of the privacy rule. This ensures that, for example, only the health care component of a hospital that has designated itself a hybrid entity for purposes of compliance with the privacy rule will be subject to the security rule. Moreover, as discussed above, the standards for the security rule mirror the categories of safeguards a hospital is required to implement under the privacy rule (i.e., administrative, technical and physical safeguards).

The AHA is concerned, however, that, because the security rule provides specific measures for the privacy rule's safeguarding requirements, hospitals will be forced to spend time and resources updating systems now, rather than having the benefit of the two years before compliance to budget costly systems changes. CMS, or the Office of Civil Rights, which is responsible for enforcing the privacy rule, should clarify and specifically address this issue. We note that because the security rule covers only electronic protected health information, such information in oral, paper or other non-electronic media will be subject only to the safeguarding requirements of the privacy rule.

At-Home Workers
In the preamble to the security rule, CMS states that "[a] covered entity's responsibility to implement security standards extends to the members of its workforce, whether they work at home or on-site." Thus, a hospital must include "at home" functions of its workforce in its security compliance plan. The use of a third-party contractor who may work from home, for example, a transcription company, will be addressed in the hospital's business associate agreement with the contractor and is not part of the hospital's security compliance plan.

Business Associate Agreements
The security rule eliminated from the proposed regulation a confusing requirement for a chain of trust agreement. Instead, the final security rule requires covered entities to "enter into a contract or other arrangement with persons that meet the definition of business associates" and "create, receive,

maintain or transmit electronic protected health information." Other analysts have suggested that the security rule requires participants of organized health care arrangements to enter into business associate agreements, contrary to the privacy rule. However, the preamble is quite clear that the security rule requires a business associate agreement only when required under the privacy rule. Specifically, CMS states that it has "adopted the concept[ ] of . . . business associates as defined in § 160.103, to be consistent with the privacy rule." Thus, hospitals will not need business associate agreements with third parties for whom such an agreement was not required under the privacy rule. Hospitals will, however, need to amend their business associate agreements with business associates that will create, receive, maintain or transmit electronic protected health information to incorporate additional security provisions required under the security rule. The AHA is concerned about the administrative burden on hospitals of having to amend their business associate agreements again.

In the preamble to the security rule, CMS also states that covered entities must make their business associates "aware of security policies and procedures, whether through contract language or other means." The AHA is concerned about the burden on hospitals of informing all business associates of the hospital's security policies and procedures and the suggestion that business associates are expected to comply with a hospital's security policies and procedures, as third-party contractors often are business associates of hundreds or thousands of covered entities—making such compliance virtually impossible. Moreover, when hospitals act as business associates of other covered entities, the AHA is troubled by the potential imposition of additional security obligations on hospitals.

Security Policies and Procedures and Training

Similar to the privacy rule, the security rule requires that covered entities implement reasonable and appropriate security policies and procedures. In addition, a covered entity is required to "[i]mplement a security awareness and training program for all members of its workforce (including management)." Although these requirements mirror the privacy rule, hospitals will be required to develop and implement additional policies and procedures and train all workforce on such policies and procedures.

Audit Trails Versus Accounting of Disclosures Requirement

In the preamble to the security rule, CMS notes that some people believe an audit trail function under the security rule will satisfy the covered entity's obligations under the privacy rule to account for certain disclosures of protected health information. CMS clarifies that, although the two requirements cover some overlapping information, "audit trails are typically used to record uses within an electronic information system, while the privacy rule requirement for accounting applies to certain disclosures outside of the covered entity." Thus, CMS cautions covered entities against using audit trails as their method of compliance with the privacy rule's accounting of disclosures requirement. Moreover, audit trails will not capture disclosures of paper records and may not contain all the information covered entities are required to provide patients in an accounting of disclosures.

Ongoing Compliance Process

The security rule provides that the security measures implemented to comply with the requirements of the Rule "must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information." Thus, compliance with the security rule is an ongoing process of reevaluation and assessment to ensure that the hospital's security measures are still reasonable and appropriate in light of new security threats and technological capabilities.