The HIPAA Security Regulations

By Terry S. Coleman, Esq., and Kimberlee C. Seah

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is known primarily for its rules protecting the confidentiality of health information, but it also includes separate requirements to ensure the physical security of that information. Physician practices that have been required to comply with the HIPAA Privacy Regulations since April 14, 2003, have also been required to comply with the HIPAA Security Regulations since April 20, 2005.¹

As a general rule, physician practices are required to

- ensure the confidentiality, integrity and availability of protected electronic health information they create, receive, maintain, or transmit;
- protect against any reasonably anticipated threats or hazards to the security or integrity of protected electronic health information;
- protect against any reasonably anticipated uses or disclosures of protected electronic health information that are not permitted or required under the HIPAA Privacy Regulations; and
- ensure compliance with the HIPAA Security Regulations by the office staff.

The regulations have three categories of standards that must be met: administrative safeguards, physical safeguards, and technical safeguards. For each standard, certain implementation specifications are required, and other implementation specifications are “addressable.”

If a specification is addressable, the practice has flexibility in whether to implement it. The practice must implement the addressable specification if doing so is reasonable and appropriate under the circumstances. When deciding what is reasonable and appropriate, the following factors are to be considered:

- the size, complexity and capabilities of the physician practice;
- the technical infrastructure, hardware, and software security capabilities of the physician practice;
- the costs of security measures; and
- the probability and criticality of potential risks to electronic protected health information.

If the addressable specification is not reasonable and appropriate under the circumstances, the practice must implement an alternative security measure that is reasonable and appropriate.

The list of standards and implementation specifications in the regulations is quite lengthy, and practices should review them in

detail. Educational materials are available on the Centers for Medicare & Medicaid Services' Web site.² The following paragraphs summarize highlights of the regulations' requirements.

Administrative Safeguards

The practice must appoint someone as the security official, and that person must assess security risks, implement appropriate security policies including sanctions for violations by the staff, and evaluate the effectiveness of the office's security procedures. Required policies include procedures for ensuring that electronic protected health information is accessed by only authorized persons and providing procedures for data backup and disaster recovery. Business associate agreements with vendors who create, receive, maintain, or transmit protected electronic health information while performing services for a physician practice must be amended to include security protections.

Physical Safeguards

The practice must limit physical access to information systems containing protected electronic health information and the facility in which they are located, while ensuring that properly authorized access is allowed. There also must be policies on disposal of computer hardware and electronic media that ensure against the inadvertent release of protected electronic health information. Software programs used by the practice should have mechanisms to ensure that transmission of electronic protected health information is secure.

Technical Safeguards

Access to electronic protected health information must be protected by passwords and other mechanisms. Practices also must have a procedure and mechanisms to access the information in an emergency.

Violations of the HIPAA Security Regulations are punishable by civil money penalties. A provider is entitled to 30 days to correct a violation without penalty, however, if the failure to comply was due to reasonable cause and not willful neglect. Therefore, it is important that physician practices appoint a security official, assess each of the HIPAA Security Regulations' specifications, and document the decisions about what is reasonable and appropriate for each of the addressable specifications.

Terry Coleman is a partner and Kimberlee Seah is an associate with the law firm of Ropes & Gray, LLP.

References

1. 42 U.S.C. § 1320d et seq. and 45 C.F.R. Parts 160 and 164, Subparts A, C and E.
2. Centers for Medicare & Medicaid Services, <http://www.cms.hhs.gov/hipaa/hipaa2/education/default.asp#SecurityEd>