HIPAA Compliance
We've Only Just Begun

by Karen S. Lovitch, Esq., and Stephen R. Bentfield, Esq.

Several significant developments have occurred in recent months related to the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the privacy and security regulations implementing those provisions. Most noteworthy was the April 21, 2005, deadline for compliance with the HIPAA Security Rule. As of that date, covered entities should have implemented appropriate safeguards to protect electronic protected health information.

Generally, the HIPAA Security Rule requires covered entities to:

- Assess the security risks with respect to electronic protected health information
- Implement appropriate administrative, physical, and technical safeguards to address those risks
- Review and assess these measures in light of new and emerging electronic security threats.

The key feature of the Security Rule is flexibility. The rule affords a covered entity "flexibility" to tailor safeguards in light of the organization's size and capabilities, its technical infrastructure, its hardware and software capabilities, and cost. Flexibility is achieved through 42 required and addressable implementation specifications.

In particular, a covered entity must have policies and procedures to ensure confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates or handles. The organization must protect against any reasonably anticipated threats to the security or integrity of such information as well as any reasonably anticipated uses or disclosure of such information that are contrary to the HIPAA Privacy Rule. Finally, the covered entity must ensure full compliance by its workforce through security training, periodic security notifications, and other means.

While covered entities are substantially complying with the HIPAA Privacy Rule, a survey revealed that they still lag behind on implementing safeguards to protect electronic protected health information under the Security Rule.[1] Overall, 91 percent of respondents (all of whom were privacy or security officials and others who work in the healthcare industry) reported that their respective organizations were more than 85 percent compliant with the HIPAA Privacy Rule standards. Only 17 percent of respondents reported that they were completely compliant with the Security Rule standards. While 43 percent described themselves as 85 to 95 percent compliant with the Security Rule standards, 26 percent reported being about 50 percent compliant and 12 percent were less than 50 percent compliant.

Entities that have yet to comply fully with the HIPAA Privacy or Security Rules can take some comfort in knowing that the U.S. Department of Health and Human Services (HHS) does not plan to take a punitive approach to enforcement. As explained in the proposed enforcement rule published in the April 18, 2005 *Federal Register,* HHS intends to promote and encourage voluntary compliance with the HIPAA rules through education, cooperation, and technical assistance, rather than through heavy-handed enforcement measures.[2]

According to the proposed regulations, enforcement activities typically arise as a result of complaints filed with HHS's Office of Civil Rights (OCR). Following receipt of a complaint, the OCR conducts an investigation and usually works with the targeted entity to resolve potential violations informally at the earliest stage possible.

The proposed rule also includes an important clarification on business

PHOTOGRAPH/PICTUREQUEST

associate agreements. It states that a covered entity is *not* liable for a business associate's HIPAA violations as long as the entity has complied with the business associates rules. An entity *is* responsible for the violations of other agents, including employees.

If the complaint is not resolved informally, HHS may impose a civil monetary penalty of up to $100 per violation, and no more than $25,000 for identical violations during a calendar year.

In the end, compliance efforts should be ongoing. For instance, a provider adopting an electronic medical records system must consider the interplay with HIPAA's Privacy and Security Rules, as recommended by the June 2004 report issued by the President's Information Technology Advisory Committee.[3] Covered entities must continually monitor implementation and, if necessary, revise policies and procedures to reflect changing needs and technological developments.

Karen S. Lovitch, Esq., and Stephen R. Bentfield, Esq., are with the Washington, D.C., law firm of Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.

References

[1]American Health Information Management Association. *The State of HIPAA Privacy and Security Compliance.* April 2005. Available online at: www.ahima.org/ marketing/email_images/ 2005PrivacySecurity.pdf. Accessed May 18, 2005.
[2]HIPAA Administrative Simplification; Enforcement, 70 Fed. Reg. 20224. (Proposed April 18, 2005).
[3]Information Technology Advisory Committee. Revolutionizing Health Care through Technology. Available online at: www.nitrd.gov/pitac/ reports/20040721_hit_report.pdf. Accessed May 18, 2005.