Health Information Compliance Alert

Reader Question: Know the HIPAA Facts on Encryption

Question: Does electronic protected health information (ePHI) have to be encrypted to be HIPAA compliant?

Codify Subscriber

Answer: Believe it or not, no - though it is certainly in the interests of any covered entity (CE) to take this, and every possible precaution to safeguard ePHI.

In "Security Standards: Technical Safeguards," the **Department of Health and Human Services** (HHS) outlines four implementation specifications for "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." Of the four, only two - unique user identification and an emergency access procedure - are required. The two others - encryption and decryption, along with an automatic logoff - are not.

Review the brief at www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.

Why? Clearly, a CE has to do something to safeguard computers, phones, or other technology that it uses to store and transmit ePHI, and encryption is ideally suited for that purpose. But if after a risk analysis the organization decides that encryption will not help it protect ePHI from "anticipated threats and hazards" in a "reasonable and appropriate way," then the entity must "implement an equivalent alternative measure," according to another HHS document, "Security 101 for Covered Entities."

See the HHS tips at www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf.

In other words, encryption is not required to protect ePHI, but it is more than just a pretty good idea.