READ THIS... STAT!

By David E. Schweighoefer

STAT! NOT TO incite panic, but this is important compliance and enforcement information that directly affects your office practice.

In 2013, significant amendments were made to HIPAA's privacy, security and breach notification rules. The rules have been strengthened, and so has enforcement.

Data breaches involving inadequate electronic Personal Health Information ("ePHI") data security accounted for nearly 80 percent of enforcement by the Office of Civil Rights ("OCR") in the past year. Consider the following:

+ A dermatology practice in Massachusetts was fined $150,000 for losing a thumb drive containing unencrypted ePHI on nearly 2,200 patients and for failing to have conducted a security risk analysis ("SRA").

+ Concentra Health Services agreed to settle with OCR regarding the theft of an unencrypted laptop containing patient ePHI. The settlement was $1,727,220.

+ Affinity Health Plan agreed to pay $1.2 million when it was discovered that the ePHI of several hundred thousand individuals was left on the hard drive of a copy machine that was not wiped clean after use.

To avoid enforcement by the OCR, physician practices and business associates of those practices are required by law to have conducted a security risk analysis. Failure to conduct this analysis may result in financial penalties by the OCR. Failure to conduct this analysis will probably result in financial penalties in the event your practice reports a data breach to the Department of Health and Human Services, as required by law.

The security rules are distinct from the HIPAA privacy rules. The security rules apply to information your practice creates, receives, maintains or transmits to others. You, as a provider, are required to identify reasonably anticipated threats or vulnerabilities and to take action to protect this ePHI from such threats. The law stipulates that some actions are required and others are considered addressable, meaning that you must be able to show documentation that indicates you have examined the specific requirement and implemented compliance with it as reasonable and appropriate.

The security rules are organized in three categories: administrative, physical and technical. Administrative safeguards require you to establish a security management process and implement policies and procedures to prevent, detect, contain and correct security violations. Physical safeguards are required and addressable standards that are designed to provide facility access controls to limit physical access to your electronic systems and the facilities in which they are housed. Technical safeguards are those required or addressable standards that refer to the technology and the procedures for use of the technology to protect the ePHI and control access to it. These safeguards protect your patients' ePHI by allowing access only to individuals or software programs that have been granted access rights to the information.

The security risk analysis assists you in identifying risks as either external (e.g., a "threat") or internal (e.g., a "vulnerability"). The security risk analysis also further helps you to determine if the risk is "likely", as well as the impact of the risk on continued operation of your practice.

Security risk analysis — highly recommended treatment for physicians everywhere.

David E. Schweighoefer is an attorney and Partner, Health Care practice group, at Brouse McDowell in Akron, OH.