Health Information Compliance Alert

HITECH Act: Heed These Enhanced Security Requirements

If your practice or facility has started using health information technology (HIT) to support the electronic sharing of clinical data among health care providers, then you need to be wary. The HITECH law which was enacted on February 17, 2009, as part of the American Recovery and Reinvestment Act of 2009, expanded the current privacy and security requirements under HIPAA.

"The provision about reportable breaches as those in which the data is unsecured (unencrypted) is one of the major enhancements of security in the HITECH Act. Other provisions of note include bringing HIPAA Business Associates -- those who perform services for covered entities such as health care providers and health plans -- under the direct jurisdiction of the U.S. Department of Health and Human Services with regard to compliance with the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule," **Kenneth Rashbaum, Esq.** of Rashbaum Associates, LLC, New York tells **Eli**.

Would a health provider mailing himself/herself patient records be technically a security breach? Not exactly, advise experts. "A physician emails something to his or her home email account, say an office chart, to finish the day's entries from home. There would be no breach of security unless the transmission was intercepted or there was another type of unauthorized disclosure (i.e., the laptop or other device from which the records were sent or to which they were received was lost)," says Rashbaum. You just need to be certain that the home computer is secured and that there cannot be accidental disclosures when family members are in the room.

"Even if the transmission was intercepted or the laptop or device was lost, the breach would not be reportable, and notification requirements need not be commenced, unless the records were not encrypted in transmission or, in the case of the lost laptop or storage device," Rashbaum clarifies.