

ENCRYPTION: IT'S A NO-BRAINER

Encryption is a very simple solution that can help healthcare organizations avoid some of the major causes of large breaches being reported to HHS, says **Susan McAndrew, JD**, OCR's deputy director for health information privacy. Laptop computers, desktop computers, and portable electronic devices are among the top media types responsible for major breaches, she added.

With encryption, you're faced with the loss of property rather than the loss of data, said McAndrew. You might not be able to prevent thieves from breaking in to offices, homes, or vehicles, but you can encrypt your PHI.

The theft or loss of PHI accounts for two-thirds of all the major breaches involving 500 or more patient records reported to HHS, said **David Holtzman, Esq.**, OCR's health information privacy specialist.

"This is astounding. This is a no-brainer," Holtzman said. "We need to encrypt."

Encryption can be a safe harbor that eliminates the need to send data breach notifications, but healthcare organizations still need to be aware of various risks. Organizations should take note of the following concerns associated with encryption, said **Dan Steinberg, JD, CIPP/G, PMP**, lead associate at Booz Allen Hamilton, based in Rockville, MD:

- **Wireless encryption.** Staff members might be using personal devices as a security work-around, which can be difficult to detect, Steinberg said. Individuals need to know the risk this creates, and a covered entity needs to know whether staff members are using personal devices.
- **Mobile devices.** This includes laptop computers, flash drives, telephones, and tablets. Don't forget about access management and automatic logoffs, along with security awareness and training. Dispose of these devices carefully and ensure that they are wiped clean of any PHI.
- **Encryption of database fields and partial encryption.** HIPAA sets out standards for "de-identification" of records. De-identified records no longer contain information that can be characterized as PHI. However, the remaining data may be used for data mining or breaking the encryption code.

Finally, remember that encryption needs to be part of a larger, robust privacy and security program, said Steinberg.