Health Information Compliance Alert

TECH TIP: 5 COMMON METHODS TO GIVE STORED PHI THE BOOT

The security rule doesn't stop you from throwing your hardware into the scrap heap, but if any of your patients' PHI is discovered on those machines, you could be slapped with a HIPAA violation.

Important: The rule mandates that you take reasonable and appropriate steps to protect your patients' confidential information. That means you could be in the clear if you can show that you did what you could to scrub hard drives of PHI before you passed them along.

Try one of these methods for erasing all data on your computers and other devices. Be sure to include use of your removal method of choice in your policy and procedures as proof that you've taken your responsibility seriously.

Symantec's Ghost - G-Disk. Pro: Provides on-the-fly formatting along with high-security disk wiping. **Con:** May not perform the same on each machine.

Darik's Boot And Nuke (DBAN). Pro: Very user-friendly, provides several techniques for sanitizing hard drives. **Con:** Takes about four hours to complete.

Eraser. Pro: Free software that allows you to overwrite data on your hard drive using either default or customized methods. **Con:** Only compatible with certain Windows operating systems.

WipeDrive. Pro: Supports any size hard drive, verifies that your data has been erased and can import overwritten files into other applications. **Con:** Can only be run on one machine at a time.

Practical Security Associates - SMART SDR. Pro: Can schedule automatic overwrites, performs a full hardware configuration scan and verifies that your data has been erased. **Con:** Does not offer extensive reporting for documentation purposes and is designed for small businesses.