Eli's Rehab Report

HIPAA Landmines: Is Your Multifunction Printer Harboring ePHI?

Keep a printer with a large memory out of bounds for unauthorized individuals.

Facilities can face an unexpected HIPAA risk if they have a multifunction printer that also sends faxes, scans and makes copies of reports and assessments for their therapists. The information technology (IT) team might suggest that you should disable the machine's ability to store information to avoid any PHI leaks. The question remains, "Is this necessary under the security rule?"

It depends. In Section 160.103, the **Department of Health & Human Services** knocked basic paper-based fax machines out of the security rule because the information being exchanged did not exist in electronic form before the transmission. But that exclusion doesn't apply to fax machines that have a hard drive or are part of your network.

Your multifunction printer's large memory doesn't push you into security rule territory. If your machine's memory can hold on to a week's worth of PHI, however, you should take steps to keep that information out of unauthorized hands.

Try this: Limit don't disable the amount of information your machine can store. Multifunction printers with permanent storage capabilities, such as a hard drive, do fall under the security rule and the information stored on them must be protected just like any other electronic protected health information (ePHI).

Good idea: Set your multifunction printer to erase stored information at the end of each day or week, Markette suggests. And you should program the machine not to print out reports containing stored information at the press of a button.

Bottom line: Do a risk assessment of the machine before you decide which rule should apply.

Strategy: Kick off your risk assessment with these questions:

- How much storage does my multifunction printer have?
- Is it also a network storage device?
- How long is information stored on the machine?
- How is stored information accessed?
- Where is the printer kept usually?
- Is it accessible by the public at large?

And remember, even if the security rule doesn't apply, the privacy rule still mandates that you protect all machines in your office from inappropriate use and access.