Codify
BY AAPC

Health Information Compliance Alert

Security: Don't Duplicate HIPAA Violations: Secure Your Digital Copiers Now

Avoid major security risks with these tips.

If you're using a digital office copier in your work place, each copy you make could add up to thousands of confidential health records inside the machine's memory. Don't worry, though: Securing that data is a breeze with a little advice from **Eli's** experts.

The basics: Many modern copiers are networked digital multi-taskers, capable of printing, copying, scanning, faxing and more. To achieve this level of productivity, these multi-functional devices (MFDs) are equipped with memory and/or a hard drive, similar to your PC, says **Vince Jannelli**, senior manager of solutions marketing for **Sharp Electronics**.

Warning: As a result of the vast amount of data that can be stored inside these copiers, information lingers long after a copying or printing job is completed. "When these devices move from one department to another--or they're either returned when their lease expires or sent offsite for repair or upgrade--confidential information moves with [them]," notes Jannelli.

Additionally, confidentiality of PHI can be compromised if a member of your staff accidentally-- or, perhaps intentionally--retrieves documents sitting in the printer's output tray. "It's not uncommon for [an] authorized user to print a confidential document and then get sidetracked on the way to retrieve it. It can be nearly impossible to keep that data secure unless precautions are taken," warns Jannelli.

Take action: These three steps will help you safeguard your patients' PHI:

- Implement a feature that requires users to stand at the copier and enter a PIN code to allow confidential documents to print.
- Restrict access to the device by securing the copier's network interface.
- Insist that a low-cost software option be installed on your digital copier. This option is designed to digitally "shred" information after every copy, print, scan or fax job.

More tips: Make these additional pointers part of your staff training on digital copier procedures.

- In general, implement physical security commensurate with that for other e-PHI storing or transmitting systems.
- Strictly observe media controls, and don't let vendors with maintenance contracts remove the disks. They should be wiped clean by internal personnel prior to release to vendors, or just destroyed if broken.
- If the device moves scanned, copied or faxed data to a network share for later retrieval by the end-user, or if end-users directly connect to the MFD to retrieve data, ensure that the data is securely transmitted and stored. Older MFDs have no protection at all.
- Vendors are getting better, but be sure to validate their security claims. "We've found that the marketing specs commonly are not correct in terms of security. Some vendors just haven't given security a second thought," notes Fred Langston, senior principal consultant with Guardent in Seattle.
- Assess the operating system patching and maintenance procedure for the device. Some devices allow you to reinstall whatever operating system you want on the systems with no checks. Others use proprietary interfaces that mitigate that risk.

Lessons Learned: "In essence, you need to treat MFDs just like any other e-PHI storing or transmitting system, advises Langston, who conducted a security assessment of different vendors' MFDs and found that each had significant vulnerabilities. "Some devices actually had multiple data storage devices-- hard drives and flash drives that captured

data. Other vulnerabilities included completely unsecured data transfers to shared network drives for scanner and FAX functions." Ask your IT professional to determine your security risk pertaining to digital copiers.