

## Data breaches may lurk in office copiers and printers

January 10, 2011

It's a common practice for many physician offices to scan copies of patients' insurance cards, Social Security numbers and driver's licenses and keep them on file.

Throwing those copies into a trash bin would be considered a violation of patient privacy. But physician offices could be putting that patient data at just as much risk when it comes time to replace the copy machine.

Office printers and copiers are often overlooked as a major source of personal health information. This is probably because a lot of people are unaware that many printers and copiers have a hard drive, just like your desktop computer, that keeps a file on every copy ever made. If the drive falls into the wrong hands, someone could gain access to the copies of every Social Security number and insurance card you've copied.

"The important thing to remember is these devices are digital, like PCs," said Larry Kovnat, product security manager for Xerox. "The reasons why they wouldn't just throw out a PC, they have to treat copiers the same way."

In April 2010, CBS News reported on a New Jersey warehouse that was storing more than 6,000 used copiers that were intended for resale but were full of private information that had not been stripped. As a result of the investigation, Affinity Health Plan, a nonprofit managed care plan serving the New York metropolitan area, was forced to report a HIPAA violation to the Dept. of Health and Human Services. The plan also notified 409,000 of its members of the data breach, even though no evidence was found that the data were misused.

John Shegerian, chair and CEO of Electronic Recyclers International, a Fresno, Calif.-based e-recycling company that runs seven recycling plants across the country, said he got into the business of recycling electronic equipment for environmental reasons.

"Now what's taken center spotlight is privacy issues," he said. "From cell phones to laptops, from desktops to printers and copiers, they all have to be handled not only for environmental best practices, but also best practices for privacy."

Kovnat said the first step is checking to see if your printer or copier has a hard drive. Machines that serve as a central printer for several computers generally use the hard drive to generate a queue of jobs to be done. He said there are no hard and fast rules even though it's less likely a single-function machine, such as one that prints from a sole computer, has a hard drive, and more likely a multifunction machine has one.

Kovnat said searching online for the make and model of your machine will probably help you find the answer. Most manufacturers and vendors will have information on each model available on their websites.

Robert Siciliano, CEO of IDTheftSecurity.com, an online identity protection consultancy, said the next step is finding out whether the machine has an "overwrite" or "wiping" feature. Some machines automatically overwrite the data after each job so the data are scrubbed and made useless to anyone who might obtain it. Siciliano said most machines have instructions on how to run this feature. They can be found in the owner's manual.

There are vendors -- many times the vendor from which you bought or leased the copier -- that will do it for you when your practice needs help. Though it's something that can be done on a semiregular basis, overwriting is something that should be done at the least before the machine is sold, discarded or returned to a leasing agent, experts said.

Shegerian said most vendors sell parts to other vendors. For example, his company takes machines apart and sells different materials to different companies, such as copper smelters and glass recyclers. The parts are sold after the hard drives are removed from the machines and shredded. He said reputable vendors should be able to supply an audit trail of the downstream vendors upon request. If they can't -- or refuse to -- provide the audit, that should be a red flag.

Kovnat said the companies should be able to provide you with a certificate of destruction for any hard drives they destroy.

Electronic Recyclers International runs a website, 1800recyclers.com, where users can choose the type of product to be recycled and the website will direct them to a recycling center.

Another resource is ISRI.com, which is run by the Institute of Scrap Recycling Industries. The website certifies recycling centers that meet industry best practice standards. It has a marketplace section on its websites where vendors can list their services.

Because of the attention to privacy issues, the vendors where you buy or lease any electronic equipment should have a plan in place for handling these issues, experts said. Whether the hard drives are destroyed or returned to you for safekeeping, it's up to you to find out. Otherwise, you could find yourself in a predicament similar to Affinity's, and have a data breach that must be reported to HHS.

Original URL: <http://www.ama-assn.org/amednews/2011/01/10/bica0110.htm>