amednews.com
THE NEWSPAPER FOR AMERICA'S PHYSICIANS

BUSINESS

Deleting computer files not enough to ensure privacy

An Alabama man's purchase of a used computer with patient records is a cue to take care when disposing of equipment.

By Tyler Chin, *AMNews* staff. April 18, 2005.

A man in Cottonwood, Ala., snapped up an old computer at a flea market for $10 and was surprised to find it chock full of personal medical information about more than 3,000 people, including his late grandfather.

The episode illustrates how important it is for doctors to scrub all personal or medical information from their old computers or risk public embarrassment and a potential pile of legal trouble.

With this article
- See related content
- Regional news: South

Records discarded with a computer could, for example, violate not only the 2-year-old federal medical records privacy rule but also a regulation that goes into effect April 20 aimed at protecting the security of such data, said Tom Walsh, a Kansas-based consultant on security issues related to the Health Insurance Portability and Accountability Act of 1996.

Under the latest security rule, physicians will be required to safeguard the confidentiality, integrity and availability of electronic health data or face potential civil and criminal penalties. Doctors also could find themselves liable to actions by patients, especially if data retrieved from a discarded computer are used to steal peoples' identities, Walsh said.

"I don't know any small physician practice that could stand to get sued for not protecting data used for identity theft," he said.

It was the potential for identity theft that struck Shawn Peterman, a self-described "computer geek," as he peeked inside the machine he bought March 6. When he booted up the old DOS computer, a program called "Doctor's Office Manager" popped up.

A few keystrokes later, Peterman said, he saw names, addresses, Social Security numbers and other personal information of more than 3,000 people who had been patients of Dothan (Ala.) Pulmonary Specialists, a small practice that is no longer open. The computer also contained the medical records of two patients, he said.

"My first thought, of course, was, 'Oh, look at this,' figuring I'd delete it," Peterman said. But upon recognizing the clinic, he typed in the name of his grandfather, who had been a patient at the practice. Up came his grandfather's personal information, Peterman said. Not knowing what to do, he contacted the *Dothan Eagle*, which first reported the story on March 10.

The names of the practice's two primary physicians -- as well as the names of 344 referring doctors -- were on the computer, which apparently had last been used in 1995.

Greg Shields, MD, one of the pulmanary practice's doctors, did not return a call to *AMNews* but told the *Dothan Eagle* that he didn't know how the patient information survived in the computer that turned up in a flea market, because the practice made efforts to delete those data.

Hiding in plain sight

But simply deleting files does not mean that those files are purged forever, experts say.

"When you do a delete, delete really equals hide," consultant Walsh said. "I don't think [physician offices] understand that doing a delete does not actually remove anything. It just makes the space where the data was on that hard drive now available for other data to be written into that space. But the 'deleted' data are still there somewhere."

To permanently erase information from a computer and make it irretrievable, doctors can either destroy the hard drive or use software utilities to "overwrite" the data in the hard drive. "When in doubt, they should hire somebody who knows what they are doing," Walsh said.

John Halamka, MD, chief information officer of CareGroup Healthcare System and Harvard Medical School, echoed those recommendations. CareGroup follows three procedures, which many doctors could adapt to their practices, to ensure that patient data are permanently erased:

- Run a software utility that reformats the hard drive of a computer, wiping it clean of clinical information and enabling the health system to "repurpose" the machine for nonclinical use within the organization. CareGroup uses Symantec Ghost from Symantec Corp.
- Ship computers to Dell Corp. if they are no longer needed but still could be useful to schools and charities. The company offers

"asset recovery services" and puts the hard drive through an "overwriting or data cleansing process that's more rigorous than what we do internally," Dr. Halamka said. "There's actually a [U.S. Dept. of Defense] standard for wiping a hard drive clean," he said, and Dell follows that protocol. CareGroup pays $20 per workstation.

- Dispose of computers that can't be reused or donated. CareGroup uses a disposal company that physically destroys the hard drive by thrusting a four-inch spike through it. CareGroup, whose flagship hospital is Boston's Beth Israel Deaconess Medical Center, pays 25 cents per hard drive, plus a 3% energy surcharge and $50 transportation fee for each pickup, Dr. Halamka said.

"You're never going to find a computer at a garage sale with Beth Israel Deaconess Medical Center data on it for sure," Dr. Halamka chuckled. "To me, there are two laws we have to adhere to. One is HIPAA, which of course makes it illegal for us to share such data. The other is the *Boston Globe* test. Wouldn't it be truly devastating to have a *Boston Globe* headline that said 'Beth Israel Deaconess data found on used computer'?

"Ultimately, I want to protect our patients' data."

Back to top.

RELATED CONTENT *You may also be interested in reading:*

Medical records security: HIPAA's 3rd deadline not a charm April 18
Safeguard records to comply with HIPAA security rule Column Jan. 3/10
Physicians being targeted in identity theft scheme Jan. 31
Industry moves on HIPAA standards, but transition will be slow Nov. 15, 2004
Penalty for breaking HIPAA law Column Sept. 20, 2004
Data guard: The next HIPAA mandate May 10, 2004