Health Information Compliance Alert

Security: 'Scrub-A-Dub-Dub': Sanitize Your PHI

Take the sledgehammer approach if need be, experts advise.

Covered entities, be forewarned: If state organizations or others are hungry for your donated computers, you'll need to take several bytes out of your hard drive before you hand them over.

It's happening more and more often these days. Health care organizations with outdated or obsolete personal computers are giving them away to other facilities without properly sanitizing their machines. Confidential health care data winds up in full view of those who shouldn't have access to protected health information, and thousands of patient files are one click away from public exposure.

Remember, CEs: You're responsible for the integrity and security of the PHI you maintain under HIPAA's security reg. If you're considering donating your computers to anyone, you need to ensure that PHI is no longer contained in any of those hard drives.

While the 1998 proposed security rule didn't clearly address how to dispose appropriately of media or systems that might have electronic PHI on them, the final rule explains what your responsibilities are, according to **Cynthia Smith,** Senior Manager at **PricewaterhouseCoopers.**

Smith said CEs must review how they're disposing of media, from floppy disks to CDs to hard drives, and how they're disposing of information that's no longer useful.

Option 1: Secure Delete. While many CEs believe deleting files will quickly and efficiently erase all PHI, "Just simply deleting data is not sufficient protection," Smith said, adding that one should perform an overwrite to properly dispose of confidential information. "There needs to be some thought on this issue to ensure that [PHI is not turned over] to a voluntary organization like a school and can be reused," she urges.

Others say that computers just don't understand that deleting files means we humans want something completely erased. "Instead, when you tell your computer to delete a file, it thinks that it should merely hide that file from you," says **Rick Edvalson,** business manager for **IntegriNet Solutions**, Inc. in Boise, Idaho.

Edvalson tells **Eli** that when a computer "deletes" a file, the name of the file is merely altered in a way that removes the file from the directory of files. It also tells the computer that the space the file occupies is now available for storing other material. But if the computer doesn't put anything in that space, the content of the "deleted" file will remain on the hard drive forever. "Someone with software tools that are commonly available could still find it and read it," he warns.

Edvalson says if CEs want to ensure that "deleted" files cannot be recovered, they can obtain software that complies with the **Department of Defense** standard. "Such 'secure delete' programs will be able to completely erase one file at a time," he says, adding that some "secure delete" programs can be found at places like **East Technologies**, software sites tucows and **ZDNet** Downloads, and many others.

Forget Deleting, Use A Sledgehammer

Option 2: Hard Drive Destruction. But for those who don't want to take the chance that some of their stored PHI could get loose in public, they may want to consider physically destroying the disk.

That's what **Fred Langston** advises, Principal Consultant with **Guardent** in Seattle. Langston is aware that sounds a bit overzealous, but stresses that it truly is the best way to ensure PHI doesn't get out on the street. "Literally taking a hammer to it until it's in little, tiny pieces. That's probably the best way."

Warning: Reformatting is no solution. If destroying your hard drives outright doesn't appeal to you, you can always go with byte-for-byte overwrites, says Langston, or what are known as "triple wipes" of the disk. He says there are many "secure delete" programs out there that will perform these tasks. Whatever you decide, Langston advises CEs to refrain from performing a simple reformatting. "A lot of people think they'll just reformat the disks and that'll fix it. That makes it so that you can't recover your operating system, but the data potentially can still be called off there; it's not as good as doing a secure byte-for-byte overwrite or a triple wipe."

Langston says that under the media and data controls of the physical safeguards included in the security rule, you are required to have in place disposal procedures that describe when you either throw data such as hard drives in the trash, or when you donate it to charity or put it on **ebay** to resell it.

He says it's required of you to have a set of procedures in place that enables you to properly explain what you're doing to ensure that data has been completely removed from your media unit.

Better To Deface Than Erase

Many people feel that erasing PHI from their disks will solve all of their problems, when that's just not entirely accurate, Langston says. That's not a complete solution, he claims, because when you open a Microsoft Word document that may contain PHI, it creates temp files.

For example: When you open a Word document, potentially there are eight individual temp copies of that document when it's opened. So, in most cases, it's best to wipe that disk completely from end to end, because there can be multiple copies of data on a system.

But for those who don't want to take chances on triple wipes or byte-for-byte overwrites, a sledgehammer can be your best friend. What it really comes down to is final and complete sanitizing of your disks. As Langston recommends, just "pull the disk drive out and take a hammer to it."