Health Information Compliance Alert

Privacy: Maintain Your Privacy With These Safeguards

Health system puts over a million records at risk.

If you've been putting privacy compliance on the backburner, it's time to bring it up front again, because investigators are paying attention, and you should, too. Last month, officials of a health system in Connecticut announced that an unencrypted hard drive with about 1.5 million patients' information on it was stolen, potentially subjecting that protected health information (PHI) to abuse. (This news featured in the January 2010 issue of Health Information Compliance Alert. Or, you can read Connecticut attorney general **Blumenthal**'s office's press release on this case posted at: www.ct.gov/ag/cwp/view.asp?Q=453916&A=3869)

Stories like this are certainly eye-catching -- and add to that the new focus in privacy with the introduction of the HITECH Act -- and you can be sure that patient privacy is gearing up to take center-stage. And with employees taking work home and bringing laptops or cell phones with them to the office, you should be sure that your office's security is tight.

Encryption is a Best Practice

If you want to give your data a fighting chance of staying private, you should consider encryption -- even though the government doesn't require it. "The HITECH Act does not require encryption, but a provision of the act addresses breach notification," says **Michelle Wilcox DeBarge,** Esq., with **Wiggin and Dana LLP** in Hartford, Conn. "Under HHS regulations, there are obligations to notify the patient, as well as HHS and the media in some cases, if a patient's PHI has been breached," DeBarge says. "However, if a breach occurs and the data was encrypted, the breach falls under a safe harbor, meaning that no notifications are necessary. Therefore, even though the law doesn't require encryption, it can help you avoid a lot of problems."

Tip: "By all means, encryption is by far the recommended means for protecting information on hard drives, especially removable hard drives and other media, such as USB keys, CDs, or any other type of medium that can easily be transported outside the organization," says **Gregory Michaels,** director of security and compliance solutions at **BluePrint Healthcare IT** in Cranbury, N.J.

Don't Stop With Individual Files

If you're already encrypting your data, you've taken a great step -- but if you're encrypting only certain files, you may be falling short of ensuring complete privacy. "Any provider who is using their machine with access to PHI or any information that can be used for identity theft really should have the entire hard drive encrypted," says **Peter Courtway**, chief information officer for **Danbury Health Systems** in Connecticut. "It's commercially available, and it's not expensive."

Avoid easy passwords: Once you go to the trouble of encrypting your hard drive, don't compromise the data by using passwords that are easy to hack, Courtway says. "Let's say your drive is completely encrypted but instead of having a password that's complex, you have one that's the name of your dog or child -- that's really the first thing that someone would try if they came across it," he says. Instead, he recommends using "strong passwords,"which involve a series of letters, numbers, and/or symbols.

Keep an eye on removable media: If you are backing up a file from your laptop and it's encrypted there, just copying it onto a USB key or CD or backup drive does not automatically keep the encryption, Courtway says. "So you must take the necessary steps to encrypt the hard drive and/or the USB key."

Best practice: If data is being shared with offsite entities, such as billers or records management companies, each

piece of removable media should have its own password. "At our organization, we had everyone turn in their USB key drives and we replaced them with drives that forced encryption to ensure that everyone is encrypting their data," Courtway advises.

Key: Ensure that your organization has policies in place keeping PHI private. "It's essential that an organization include in its privacy policy that any type of PHI can only be on removable media or portable laptops, etc., if it's properly protected," Michaels says. "Make the employees aware of the reasons for this and try to make the employees knowledgeable."