Health Information Compliance Alert

Securing PHI: How Secure Are Your Data Management Practices?

Encryption holds the key says expert.

You're risking substantial security breaches unless you can answer some key questions about your data. Knowing what data devices are in use and whether they are fixed or portable, approved or not, are just some of the questions you will need to answer, cautions **Jim Sheldon-Dean**, Director of Compliance Services, Lewis Creek Systems, LLC in Charlotte, Vt.

"Preventing a breach depends largely on securing the various devices that hold the data, by password protection and encryption," says Sheldon-Dean. You need to do a thorough analysis of your data flow so you can discover all the places it can be stored or transmitted. "Once you know where your data is located and what devices are in use, you can make sure the data on those devices is secured," he adds.

Read on for more expert advice on how to protect your data security systems from costly flaws.

Tighten Up on Data Access

Track who can access or modify information. For example, a patient's medical records may be viewed by multiple providers, including the consulting physician and the pharmacist. Once you know who is supposed to have access to the data, assign passwords. Using passwords to protect data automatically limits access. "The regulations require individual login IDs and passwords for access to electronic systems holding PHI," affirms Sheldon-Dean.

Secure Old Data

Protect your old data by keeping a backup of survey and audit records. Put into place regular procedures for data backup and recovery and record backup details. Make a call on which old data you can safely destroy and which you need to preserve. There should be standard procedures for data deletion/destruction.

"I recommend contracting with a high-quality, reputable document destruction company that can handle both your paper and media needs, including shredding of old CDs, DVDs, memory modules, hard drives, and any other devices being retired that need to have data purged from them," says Sheldon-Dean.

Encrypt Portable Devices

"The number one cause of breaches is the loss or theft of portable devices, such as laptops, memory sticks or thumb drives, smart phones, and CD/DVD/tape media," says Sheldon-Dean. Data theft from stolen devices could be avoided through encryption, so that any information held on them would be useless to criminals and protected from breach notification requirements.

And encryption safeguarding applies to backed-up media, too. "All backups, because they are done on portable media, and because they are being stored electronically offsite, should be encrypted using encryption that meets the HHS guidance for safe harbor from breach notification," says Sheldon-Dean. "Backup tapes get lost or stolen routinely and must be encrypted to prevent potentially huge breach notification costs," he adds.

"The moral of the story," says Sheldon-Dean "is that if the device holding the data can grow legs, it needs to be encrypted to prevent breach notification."

Train Your Staff

The effectiveness of your security management process will depend on frequent reviews of your policies. Make sure all staff, even temporary employees, are trained on your security procedures, says Sheldon-Dean.

Information security management process policy hinges on the success of risk assessment and analysis --" and staff training is vital.

Document Your Work

Document your information security actions and training to show that you have policies in place and that your facility is following them. This documentation of policies and procedures must realistically represent actual practices being followed within your practice and must be within regulatory requirements, points out Sheldon-Dean.

Your contracts with third parties should require meticulous documentation of the information system access and outline the user management policy of your facility or practice, advises Sheldon-Dean. This would help reduce the risk of accidental disclosures by third parties.

Remember that this very documentation of restricted access, data encryption and control of physical access will help demonstrate your compliance.