Health Information Compliance Alert

Security: Start 2008 By Tightening Up Your Electronic Data Safeguards

7 system checks keep your data safe and sound.

Your old data protection plan may not be enough to shield you from all the new threats to your practice's vital electronic information. If you're not careful, your healthcare practice could become another in the growing list of those that have lost vital information to some unknown intruder or even an office insider.

To avoid data theft or loss, nationally known healthcare attorney **Wayne J. Miller**, speaking at an **Eli**-sponsored audio conference on HIPAA rule compliance, advised adopting some simple strategies to help you save your data.

"Little things like password protection and higher levels of encryption may be very helpful in adding security, as well as a good defense in the event of an unexpected or large incidence," he asserted.

Scary scenario: Miller told attendees about a health plan whose subcontractor sent the protected health information of 75,000 patients on a disk using a commercial overnight carrier. The disk was lost in the transition and all the PHI with it. The loss and the lack of proper care in password protection led to severe repercussions for all parties. "This is how little things become big and change into expensive things," said Miller.

Target Your Practice's Most Vulnerable Areas

Security weak spots include all your communication and use of data outside the office, your internal network for transmitting patients' electronic records, your Internet browser and the office computers. And don't forget employees' home computers, along with the Smartphone, the BlackBerry, iPods, and other devices employees use to work outside office.

Data corruption is another security vulnerability, Miller warned. If data becomes damaged or messed up, every bit of the record is completely lost. "You have to think about security as not just keeping the bad guys out but also maintaining the data in its actual format with all the information easily accessible when needed," Miller advised.

What would happen next? If you do not adhere to security issues and do not have a good backup system, you could face severe penalties under the HIPAA rule, the Fair and Accurate Credit Trade Act, and government agencies like the **Centers for Medicare & Medicaid Services** (CMS). Besides hefty fines, your reputation could be severely damaged by the loss of patients' protected health information, as well as their Social Security numbers and other financial-related information. The public would discredit you, even if the a subcontractor had committed this blunder, putting you in an embarrassing situation.

Protect Your Data With These 7 Checks

Reviewing the HIPAA rule's security components below is the first step toward ensuring safer data. "The idea of these regulations is that you look at it from the perspective of the size of your practice and the money you have to spend" on data protection, offered Miller.

Security Requirements: Make sure you're following the computer security standards in the HIPAA rule. For instance, you must have password protection facility and use it religiously and document what you're doing. "How you comply with these security regulations and what approach you follow that should be considered," said Miller. So, if audited, you should have all the security levels and methodology in compliance with the laws.

Administrative Requirements: This includes your paperwork and security protocols. Once the procedure is laid down, you must ensure that it is properly communicated to your staff. Staff should be aware that if they want to look at the medical records, they have to go through the medical record program along with a series of steps, passwords, no duplicate data to take home and so on, advised Miller.

Keep staff updated on any new security upgrades and provide them with a simple, concise and realistic contingency plan protocol. The emergency plan should include a team that responds swiftly when there's a security breach, each performing their duties as outlined in the plan. "The emergency plan doesn't have to be a 50-page plan, but it could be a contact tree containing information like a backup program."

Physical Safeguard Requirements: According to the HIPAA rule, there should be a proper demarcation on public-access areas and non-public access areas to avoid the public from seeing secret information on your computers or your laptops. There should be good security in terms of alarms, which would lessen the likelihood of theft. You can keep your computer under lock and key, but if you have good access controls, there is less likelihood of a breach, advised Miller.

Technical Safeguard Requirements: "This works as the last line of defense, and if everything fails, you should have something on the computer that's going to provide security," said Miller. The biggest problem Miller encounters is that many people rely on the default security settings, which are intentionally set at low security levels.

Miller suggested going beyond the default settings of the software and using the security to the best extent one can. And make periodic changes in the passwords, using stronger passwords to prevent a breach. There could be biometric controls like fingerprints and eye scans which come at affordable rates, suggested Miller. He also advised following basic methods in off-the-shelf programs to avoid any damage.

Assessment: To comply with the HIPAA rule, there should be an assessment process. If you are using a contractor, make sure his systems are compliant and make sure all of your office's programs have enhanced encryption levels and enhanced password levels, said Miller. He recommends having a centralized database or online data storage or a virtual private network to prevent main database theft if the PDA is stolen.

Offsite Uses: These days lots of healthcare staff work outside office. Make sure they follow the same office security measures on home computers and such devices as BlackBerries and the iPods.

Tracking Ability: HIPAA recommends having proper controls over your computers or laptops. This includes tracking where documents are going, what data is being used, and what methods are permitted in using that information to give you some semblance of control once it leaves your desk, said Miller. If a data is stolen, you must find out which data has been stolen and whom it affects to help you take effective steps in mitigating the problem.

Secure employees' info: Use the same methodology to secure employees' information as that of patients to avoid liabilities monitored by other laws, especially federal laws and state laws, recommended Miller.

In the event of an audit: If a situation arises where government gets involved and feels that you did something wrong, show them the protocols followed, that your security methods meet the scalability measures and, most importantly, that you are complying with the law, said Miller.