Part B Insider (Multispecialty) Coding Alert

HIPAA: Home May Be Where The Privacy Violation Is

7 tips for dealing with work-at-home coders

Off-site shouldn't mean out of mind when it comes to dealing with private health information.

If you let your coders, billers, transcriptionists or other administrative staff work from their homes or some other offsite location, then you need to be twice as aware of potential compliance problems. "The way the [Health Insurance Portability and Accountability Act] security rule is written, it's scalable," says **Tessa Chenaille,** president and CEO of **Chenaille Compliance Consulting** in Medford, MA. "You do what you can do to protect [PHI], and if you can't protect it you can't use it."

She and other experts offer the following tips for safeguarding patient information with work-at-home coders:

1. Be prepared to spend some money for secure computers. Make sure the at-home employee has anti-virus protection on his or her home computer, says Chenaille. Obtain assurances from the employee that he or she is protecting the data.

2. If the employee takes paper files home, don't let him or her take home originals, advises **Philip Gordon**, a partner with **Littler Mendelson** in Denver, CO.

   "Whatever rules apply to paper documents in the office also should apply to paper documents at home. For example, they should be locked up when not attended by the employee," says Gordon.

3. Locked doesn't just mean a closed door, Gordon adds. It should be impossible for the employee's kids or other people to get into the room that contains the files or other information.

4. Visit the employee at home. "I would want to see the setup that they have, to make sure that other people can't get on their system," says Chenaille.

5. If the employee is accessing an internal server remotely, all of those communications should be through a virtual private network that is secure and encrypted, says Gordon. Also, any policies against emailing patient information at the office should apply at home as well.

6. If you loan the employee a laptop to work on, make sure to erase all patient information from the laptop after the employee returns it. "The physician's practice should have specific laptop policies," including a sign-out sheet and a set of rules, says Gordon. The employee shouldn't leave the laptop sitting in a locked car where anyone could grab it.

7. If you work with a billing company, make sure it's aware of HIPAA and has a compliance plan. "If you even suspect that they're violating the agreement, it's basically your responsibility to make them change their practices or to cancel their agreement," says Chenaille.