

Health Information Compliance Alert

COMPLIANCE STRATEGY: Oh No! Your Protected Health Information Is Leaking

Use this 4-step plan to plug holes in your privacy compliance program.

You can significantly reduce your practice's HIPAA risks if you follow our four-step plan. It's simply a matter of spotting and repairing places in your practice where patients' health information might leak.

Think of your practice as a big pipe. At one end, patients come in, take a clipboard, and give you health information. The health information then flows through the pipe to the doctor, who combines the patient's personal history with lab tests and physical exams to create more health information.

At the other end of the pipe, your billing office passes that health information on to insurance companies and other physicians.

HIPAA is designed to keep the flow of health information from spilling out of your practice and into unauthorized hands, explains Dr. **Lewis Lorton**, chairman of HIPAAdocs Corp. in Columbia, Md. In other words, it's about making sure medical practices don't leak.

Chances are your practice isn't watertight. "Most small practices leak information like a sieve," Lorton laments. They tend to be "very casual about where they leave information and how they broadcast it." Staff members often leave people's names on records, on notes, on lists lying around their offices in plain view.

The solution: Lorton says you don't need to impose "draconian measures" that bludgeon staff members with the dangers of non-compliance and make it difficult for them to do their jobs. Instead, the solution is a simple emphasis on the confidentiality of their patients' files. Medical practices, he counsels, "have to learn not to leave information around, not to share it casually in the halls or waiting rooms. They just need to treat patient records with the same care that banks treat financial records."

HIPAA experts recommend this four-step process for sealing potential health information leaks in your practice.

1. Locate where your practice's health information is. Look for any information with identifiers that tie it to a particular patient," advises attorney **Bill Roach** of Gardner Carton & Douglas in Chicago. For the most part, he adds, the information is in the traditional medical record, though it can also include other personalized interactions, such as the sign-in record.

2. Create a health information map. Once you understand what you're looking for, Lorton instructs, you need to look at how you handle it. He suggests medical practices ask themselves the following basic questions:

- Where do we get our information?
- Who do we get it from?
- How do we manage it?
- When it comes in, do we handle it the same way each time?
- When we send it out, do we handle it the same way each time?

- Do we know we're sending it to the right person?
- What if we send it to the wrong person?

A practice can't begin to figure out where it leaks until it figures out how and where its health information flows.

This kind of "information-mapping" shows you where your work processes allow information to escape, says **Donna Bailey**, PhD, RN, director of the Teaching Assistant Development Program in the Center for Teaching and Learning at the University of North Carolina at Chapel Hill.

"What the leadership in a medical practice needs to do is pick their top five processes, the things they do routinely," advises Bailey, who is also an adjunct professor in UNC-CH's School of Nursing. For example, a practice's most common process might be the way it handles children with head colds. "Take that process and map it out and see where the vulnerabilities are in terms of the privacy and confidentiality of patient information," she says.

3. Perform a gap analysis. Remember that in any process the information begins to flow the moment the patient enters the office. So to assess any potential vulnerabilities, you need to begin in the waiting room, Bailey says.

For example: "When you recognize that people are signing in when they first arrive, you need to ask whether that's a vulnerability" or an "incidental disclosure." That's HIPAA's term for something unavoidable and therefore permissible under the circumstances. If it's a vulnerability, Bailey says, "you need to think about the kinds of processes and technologies you have in place" that can plug the hole. If you don't have anything, she continues, you need to brainstorm.

As you brainstorm, reminds Lorton, never forget that your purpose is to minimize the amount of personal information that unauthorized people might see or hear.

This kind of "gap assessment" is trickier in a small private practice than in a large institutional one, says **Mikel Lynch**, Chief Compliance Officer for University of Missouri Health Care in Columbia, Mo. In a hospital or big practice, staff members are asked to focus on a core task and isolating information flow and individual responsibilities is much easier. In a small practice, however, the M.O. is usually "all hands on deck" and everyone wears multiple hats.

4. Educate your practice's physicians and staff. When they're complete, a practice's information map and gap assessment become a database, a way for staff members to learn how information flows through their pipe.

Bailey says having the map is as much a question of good basic organizational management as protection of personal health information. Knowing how information flows within an office makes quality improvement possible.

"When people tell me I don't have time, I tell them they don't have time not to," Bailey insists. "They need to understand their work processes anyway."

Good news: Despite people's worst fears, sometimes this kind of assessment reveals not only failures but successes, observes attorney **Michelle Kennett**, of the Michelle Kennett Law Offices in Columbia, Mo.

"A critical thing medical offices might not realize is that they're already doing a lot of the things they ought to," she notes, adding that medical offices need to "identify those things they're doing right, tweak them, and document them." "This is manageable," she says. "Even with only five people in your office, you don't need to tear down the building or do anything weird. You can work with what you've got."