# Health Information Compliance Alert

## Patient Privacy: Have Patient Data? You Can Still Travel Safely

**Just make sure you maintain your HIPAA compliance on the road.**

Protecting your clients' private medical information may seem like old hat, but breaches continue to make headlines.

Consider this: The HHS Office for Civil Rights reported 16 privacy breaches affecting at least 500 individuals in the past month and a half. On average, the OCR has reported an average of 18 breaches per month since February of last year -- and the majority of them were the result of stolen laptops or misplaced files.

Example: OCR recently fined the General Hospital Corporation and Massachusetts General Physicians Organization Inc. in Boston to the tune of $1 million after a Mass General employee left files on a subway train that were never recovered.

The last thing you need is for a staffer to accidentally expose a client's confidential information to an unauthorized\ person. And when you work with patients in their homes, your likelihood for a breach skyrockets. Use this expert advice to make sure your staff are able to keep information under wraps -- especially when they're on the go.

**Warning: Ears Are In The Room**

You can't always clear the room of your patient's family members or visitors, but you can protect yourself if and when protected health information (PHI) is overheard, points out **Lee Kelly**, senior security consultant with Fortrex Technologies in Frederick, Md.

Good idea: Explain to your patient that by having other people milling around, his PHI could be overheard. If he refuses to clear the area, ask him to sign an acknowledgement form that states he is willing to accept that risk.

In the same vein, you should never discuss others' PHI when visiting a patient's home, experts note. If you make or accept a phone call about another patient, "leave the room or limit what you say," stresses Kelly. "There's still a chance someone will overhear you, but you've done your best to protect the other client," he explains.

The only file you should have with you in a patient's home is the one you need to treat that patient, notes **Brian Gradle**, an attorney with Washington, D.C.'s Hogan & Hartson. Any other patient files should remain locked in a safe place like the trunk of your car, he says.

And if you're working from a laptop or other portable device, make sure you have only that patient's file open, Gradle says. That way, even in a worst case scenario, the only information that can be spotted by anyone other than you will be that of the patient you're visiting, he notes.

Remember: When you use a laptop -- whether in a client's home or in the office -- you have to take measures to keep the electronic PHI from inappropriate access. "Use password-protected screen savers" and set them to kick in after five minutes of inactivity at the most, Gradle recommends.

Your laptop should be kept locked up when not in use, just as you would do with your patients' paper files. You can choose the trunk of your car, a closet in your home, or a filing cabinet in the office, Kelly advises. "You want to keep it someplace where someone can't look in a window or over a counter and see it."

In patients' homes, you should probably take a little time to explain how they can keep their own information secure. "We recommend that patients keep their personal medical information in a drawer or another place that's not open to everyone," shares **Brenda Butte**, compliance director for Alliance Physical Therapy in Minneapolis.

Even if you aren't worried that your clients will expose information, teaching them "the rules" will help them better understand the precautions your staffers must take, Butte notes. For instance, if a patient knows that you are trying to keep his data safe, he'll be more understanding when you must continually enter passwords or ask others to leave the room.

**Good idea:** Use your notice of privacy practicesto initiate a conversation on how to keep medical information out of unauthorized hands, Butte advises. You can't control everything that happens in your patients' homes, but you can decrease the chances that your patients' PHI will be inappropriately disclosed, experts agree.

Plan of action: To minimize potential security breaches due to inexperience, ask a senior staff member to accompany a newer member on her first round of home visits to ensure patients are given enough information to keep their own medical data safe, Gradle recommends.

If you can't go with your newer staff to each home visit, you could try including privacy- and security-related questions on your annual patient satisfaction survey, experts suggest. This will help you find out who is slacking.