

Part B Insider (Multispecialty) Coding Alert

HIPAA : Traveling With Patient Files? You Can Still Stay HIPAA Compliant If You Use These Tips

Becoming PHI travel-savvy is especially important if you work in several locations or in patients' homes.

Protecting your patients' 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 those 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 staff member to accidentally expose a patient's confidential information to an unauthorized person. And when you work with patients in locations outside of your office, such as their homes or separate clinics, your likelihood for a breach skyrockets. Use this expert advice to make sure your staff members 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, 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 patient, he explains.

If you're working from a laptop or other portable device, make sure you have only that patient's file open, says **Brian Gradle, Esq.**, an attorney with Washington, D.C.'s Hogan & Hartson. 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, 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. Like your patients' paper files, when not in use, a laptop should be kept locked up. "You want to keep it someplace where someone can't look in a window or over a counter and see it," Kelly advises.

Good idea: Use your notice of privacy practices to initiate a conversation on how to keep medical information out of unauthorized hands, advises **Brenda Butte**, compliance director for Alliance Physical Therapy in Minneapolis.