Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

Compliance: Is Your Doctor 'Absent-Minded?' That Excuse Won't Fly With OIG

Plus: Auditors have been known to tap into hospitals' wireless hotspots from the parking lot to see if patient information is freely accessible.

Your practice has to navigate various compliance issues every single day, and it can be hard to get answers from the OIG on how to resolve specific problems. The OIG discussed many of these issues during its four-hour HEAT Provider Compliance Training session on May 17, where OIG experts offered advice on how to avoid healthcare fraud and abuse, and what to do if you find these issues in your practice.

Although the OIG reps covered a very wide range of issues during the training session, we've broken down six of the most important compliance topics that apply to Part B practices, and shared the advice that the OIG reps elucidated during the conference.

1. Don't try the "my doctor's bad at record-keeping" defense. The OIG and CMS expect your practitioner to maintain thorough documentation no matter how much he hates record-keeping. That's the only way the government has to confirm that you've coded and billed properly.

"That whole absent-minded professor thing--'I'm a good doctor, I'm just really bad at paperwork'--OIG finds that excuse neither charming nor persuasive," said **Julie Taitsman, MD,** the OIG's chief medical officer. Good medical record-keeping not only ensures that you're billing appropriately, it also promotes better patient care because everyone treating that patient should be able to see the full documentation of your patient encounter.

2. Watch out for "lease creep" problems. Most Part B practices know how important it is to stay on the right side of the Physician Self-Referral Law (also called the Stark Law), but aren't fully aware of the types of situations that the law covers. One potential compliance issue involves lease arrangements, which the OIG is watching.

"Sometimes a DHS entity like a hospital will enter into a space lease arrangement with a physician practice that refers to the hospital, and sometimes the physician may be actually occupying or utilizing much more space than is contemplated in the lease document," said **Meredith Williams, Esq.,** senior counsel with the OIG. "The result of that type of arrangement is that the rental value paid by the practice may end up being below fair market value."

Tip: Put a system in place notifying you when your leases are about to expire, and confirm that you're collecting rent properly and that the rent is fair market value for the space that's actually leased, Williams said.

3. Know the guidelines for returning overpayments. If you receive an overpayment from your Medicare contractor, you must return the overage within a specific time period. "Even if you make an innocent billing mistake, you must repay the government," Williams said. "The Affordable Care Act included a new requirement that providers must repay overpayments to Medicare and Medicaid within 60 days or be subject to penalties."

4. Mandatory compliance plans are coming soon. Although the government has not yet finalized the requirements that you'll need to follow for mandatory compliance plans, you should be aware that they are on the way.

"The health care reform law includes a requirement for providers and suppliers to have compliance plans as a condition of enrollment," said **Amanda Walker, Esq.,** senior counsel with the OIG, during the session. The implementation timeline for Part B practices has not yet been defined, but CMS has already revealed the seven elements it believes are essential to an effective compliance an ethics program, and the agency has sought comments on those elements. "While the specifics are still being ironed out through the regulatory process, we do know that compliance practices will be

mandatory soon enough. OIG has promoted voluntary compliance programs for years," she said. Following are the seven compliance elements that CMS has identified:

- Written policies and procedures for your compliance program, which you should share with all members of your organization.
- Identification of compliance professionals in your practice who are keeping up with federal and staterequirements.
- Effective training to educate your employees of your compliance policies.
- Effective communication lines between the compliance officer and the other members of the organization.
- Internal monitoring systems, such as internal audits or other reviews. "A good compliance program will identify problems from time to time," Walker said. "If it doesn't, that's a sign that what you're doing is not working. If you detect something problematic, then you're in a position to do something about it."
- Enforce standards and take action if an employee is not following the procedures.
- Prompt response to any issues that you identify.

5. CMS doesn't have to pay your claim right away if abuse is suspected. Although most practices believe that MACs and the OIG only review claims on a retrospective basis, that isn't always accurate, Taitsman said. "For suspicious providers, CMS does not have to automatically pay claims. CMS can place suspicious providers on prepayment review when they have reason to suspect fraud or abuse."

In addition, the government will be more vigilant than ever in seeking documentation to review. "Going forward, you should be aware of an increased enforcement of documentation requirements," Taitsman said. "I can point to several reasons for this. First, the administration is pursuing an initiative to cut the improper payment rate in Medicare fee-for-service in half by 2012. Second, OIG has recommended that CMS and contractors focus on error-prone providers, and CMS is increasingly tasking Medicare contractors to review medical records to prevent improper payments."

6. Ensure that your EHRs are totally secure. Electronic health records (EHRs) offer improved accessibility to providers who want to review patient charts. However, in some cases, this accessibility causes security issues, Taitsman said.

"In some of our information technology audits, we have OIG auditors who will sit in the parking lot of a hospital with a laptop computer and drop on to the hospital's wireless network and actually be able to access patient information that's supposed to be private."

Tip: Confirm that your EHRs and other systems are configured securely so that patient information stays completely confidential.