MDS Alert

Compliance: HEAT Training Session Homes in on These Key Medical Record Compliance Issues

Be aware of a crackdown in this area, says OIG official.

In a recent HEAT training session on documentation, **Julie Taitsman, MD,** chief medical officer for the OIG, warned that "going forward, you should be aware of an increased enforcement of documentation requirements."

Why: Taitsman noted that "the administration is pursuing an initiative to cut the improper payment rate in Medicare fee-for-service in half by 2012." And the "OIG has recommended that CMS and contractors focus on error-prone providers, and CMS is increasingly tasking Medicare contractors (MACs, RACs, etc.) to review medical records to prevent improper payments."

At one point in the session, Taitsman held up a copy of a page of a medical record with a highlighted diagnosis of chronic renal insufficiency, which supported services that the provider had billed. The provider highlighted the diagnosis, not the OIG, she said. And there "was no notation on this record to indicate that anything had been added" to the record later.

The catch: The OIG audit team had an earlier copy of that same page of the medical record, which didn't have the diagnosis on it at that time, Taitsman relayed. "The coverup just makes it worse," she warned. (For a free article on a backdating case that surveyors discovered in a nursing facility, e-mail the editor at KarenL@Eliresearch.com.)

Taitsman also had a message for physicians: "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. "

Got EHRs? Test for This Security Issue

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," she cautioned.

Tips: The best way to detect that problem, says HIPAA expert **Jim Sheldon-Dean**, is "to do just what the investigators do. Set up a laptop to be used as a wireless access testing tool and use it regularly and all over your facility." He notes that "this kind of a tool is cheap to set up (it uses a low-end laptop and free software) and easy to use." And "if a facility doesn't have the expertise to do this themselves, they should ask for professional assistance, as it is absolutely necessary to protect networks and all the data they hold access to by checking for open access points," adds Sheldon-Dean, principal of Lewis-Creek Systems in Charlotte, Vt.

"You can even find out a lot just by using a regular laptop with a wireless card and no special software to find and catalog all accessible networks," Sheldon-Dean advises. "Go somewhere in the facility, sit down, and see what wireless networks you can get into. Then try a different location. You may be surprised to find out how much open access there may be."

Editor's note: You can watch a webcast of the HEAT (Health Care Fraud Prevention and Enforcement Action Team) training at http://oig.hhs.gov/compliance/providercompliance-training/index.asp. See the next MDS Alert for continuing coverage of the HEAT training sessions.