Psychiatry Coding & Reimbursement Alert

Practice Management Tips: 5 Types of Audits You May Face: Be Ready Before Auditors Come Knocking

Why a letter from your ZPIC isn't good news.

You've heard the saying, "If you're not paranoid, you're not paying attention." The same thing applies to audits: If you're not worried about who could be looking at your records, you could be headed for serious trouble.

Read on for the scoop on getting ready for five different types of audits: four Medicare audits and Health Insurance Portability and Accountability Act (HIPAA) audits under the Office for Civil Rights (OCR) program to assess privacy and security.

1. Watch for ADS Letter From Your MAC

Your Medicare Administrative Contractor (MAC) processes claims and can perform pre-payment and post-payment reviews. If your MAC identifies you for an audit, it will send you an Automated Development System (ADS) letter, typically asking you to submit specific documentation.

Important: Be sure to review both the front and back of the ADS letter to ensure that you send all of the claim documentation to the MAC. Missing information could result in your entire claim being denied.

You may be asking yourself what the top improper payment culprit is that MACs see. "CMS has found that most Medicare improper payments happen because a provider did not comply with Medicare's coverage, coding, or billing rules," according to **Sherrie Varner** during a TrailBlazer Health webinar, "Medicare Documentation and Audits."

2. Focus on Post-Payment for CERT Audits

The Comprehensive Error Rate Testing (CERT) audits are exclusively post-payment reviews. "The CERT program is CMS's process to determine how accurately Medicare contractors review and process claims," Varner said.

Why does this apply to you? If the CERT finds errors involving money overpaid to your practice, it instructs your MAC to recoup the funds from you.

In addition, errors that the CERT identifies can become issues of focus in future MAC and RAC audits. A "very common" CERT error is insufficient documentation, Varner said.

3. Distinguish Automated and Complex With Recovery Auditors

Formerly known as Recovery Audit Contractors (RACs), recovery auditors perform only post-payment reviews. However, CMS is contemplating a demonstration project in which RACs will be allowed to review claims before they are paid to ensure that the provider complied with all Medicare payment rules. Under this demonstration, the RACs will conduct prepayment reviews on certain types of claims that historically result in high rates of improper payments. These reviews will focus on seven states with high populations of fraud- and error-prone providers (FL, CA, MI, TX, NY, LA, IL) and four states with high claims volumes of short inpatient hospital stays (PA, OH, NC, MO) for a total of 11 states. The demonstration was slated to begin in August 2012.

Recovery auditors can look back for three years from the date your claim was paid, but they can't review any claims paid before Oct. 1, 2007. These auditors perform two types of reviews -- automated and complex.

During an automated review, the auditor will not request medical records from you, but will instead base the review on the claim information that you already submitted to Medicare.

In the case of a complex review, the auditor will request records from your practice, which are subsequently reviewed by doctors, nurses, therapists, and coders. If documentation is missing or incomplete, the auditors might downcode or deny services, and can instruct your MAC to recoup money that was overpaid.

Pointer: When trying to prepare, you can focus on some out recently-posted RAC focus areas. Overpayments to physicians who report an incorrect place-of-service (POS) code are in the audit crosshairs. Because physicians collect higher payments for procedures at non-hospital facilities, entering the correct POS is essential to proper pay.

Another RAC audit focus area is overpayments due to providers incorrectly billing bilateral procedures on two lines -- once with modifier 50 (Bilateral procedure) (resulting in 200 percent payment) and once without modifier 50 (resulting in 100 percent payment), for a 300 percent total payment.

Do this: You should report bilateral procedures as a single line item with modifier 50. If your MAC prefers that you report the codes on separate lines, you'll report two listings of the same CPT® code, but you shouldn't append modifier 50.

4. Raise a Red Flag If ZPICs Come Knocking

The Zone Program Integrity Contractors (ZPICs) review potential Medicare fraud, Varner said. "If you get a letter from them, it's not a good thing."

Not only can the ZPICs perform medical reviews and data analysis, but they can also investigate fraud and abuse, and refer cases to law enforcement, Varner said.

5. Form a Team to Prep for HIPAA Audits

All covered entities and their business associates are eligible for a HIPAA audit. Your practice can take the following steps to be ready for such an audit:

Review what you do: A team of personnel from your practice, including (where applicable) medical records, information technology, your security officer, and your counsel, should "review all privacy and security policies, procedures, and practices, and should update and revise them as needed," says **Kenneth Rashbaum, Esq.** of Rashbaum Associates in New York. Make sure you preserve information relevant to security and privacy protocols to establish your compliance efforts.

Assess risk: Conduct and document a HIPAA security risk analysis. The U.S. Department of Health and Human Services has issued a guideline on the requirements of this risk analysis, according to Rashbaum.

Document: If you face a HIPAA audit, remember that the authorities want to help practices be compliant, not just find potential violations, according to **Jim Sheldon-Dean,** Director of Compliance Services, Lewis Creek Systems, LLC in Charlotte, Vt. What auditors will want to see is evidence of policies and procedures that you have in place as well as evidence that you are making a good faith effort to follow those policies and procedures. Even if they find security deficiencies, your documentation can show auditors that you take security seriously, which is the point.