Codify
BY AAPC

Outpatient Facility Coding Alert

Revenue Cycle Management: 7 Ways to Prevent Embezzlement in Your Business Office

Tip: Conduct outside audits every three years.

A former administrator at a surgical eye center was recently indicted by a federal grand jury for allegedly embezzling more than $500,000 from her employer, the **Department of Justice** announced September 13, 2017.

In this case, the employee was able to siphon off funds because she had access to two credit cards that she was supposed be using to pay for office equipment and supplies. Instead, she was using the eye surgery center's credit cards to pay for "her son's private school tuition, maid services for her home, entertainment, dining, high-end clothing, jewelry, and airline travel," the DOJ alleges. It was not until the employee resigned and moved out of the state that the surgery center discovered the embezzlement activities.

Employee embezzlement at medical practices and surgery centers is all too common, says ophthalmologist **James Loden**, who spoke at the recently held Millennial Eye Live conference in Nashville. Sometimes embezzlers are trusted, high-level employees who have worked at the center for years. There are numerous ways that employee embezzlers can take advantage of small, day-to-day transactions to line their own pockets, such as:

- Employee takes cash payment from patient and does not post charge or payment.
- Employee gives patient a fictitious receipt for payment that was made.
- Employee gives busy doctor or administrator a sheaf of checks to sign, and includes an extra one.
- Refund check made out to fictitious patient. (Employee has previously opened an account under that name.)
- Employee substitutes insurance check payment for cash taken and doesn't post insurance payment.
- Rubber stamp is made of doctor's signature: employee uses to make extra paycheck for self.
- Employee purposely pays a bill twice and then pockets the resultant refund.

Your business office should create policies and procedures that limit opportunities for embezzlement and protect your facility from losing the revenue it needs to stay profitable. Here are some tips from Dr. Loden and other experts:

1. Perform rigorous background checks on prospective financial personnel. Call the references, even if the candidate says, "I don't want you to call my prior boss because we have a bad relationship. If the answer you get on a reference check is something like "all we can confirm is that the person worked here," don't hire the candidate.

2. Insist on clear financial reporting, Dr. Loden urges. Overly confusing reports are very bad for business.

3. Make sure you're using all the capabilities that your ASC's inventory management system offers. Employees can make a lot of money selling devices and drugs on the black market, and sloppy inventory management makes it very easy for them to do that. A good system tracks devices and drugs from the time they are ordered until your facility is paid for the product. If your ASC is still tracking inventory manually, consider investing in a solid inventory management system to add transparency to the process.

4. Use your inventory management system to create orders based on prior history of purchase and use. This step reduces the likelihood of embezzlers over-ordering with the intent to create refunds for themselves or to sell the items themselves.

5. Look out for vendor kickbacks that encourage employees to make purchasing decisions that aren't in your ASC's best financial interest. Used medical equipment dealers are the biggest offenders in this regard, Dr. Loden warns. Kickbacks can take the form of gift certificates, sports tickets, and other perks that go directly to the

employee making the purchase decision.

6. Create access controls for your software that are appropriate to each position. For a variety of reasons (including HIPAA), employees should have access to only the parts of your EHR and facility management software that allows them to do their jobs. Customized security levels-as well as separate log-ins for each employee-let you define what areas of your systems employees can access and what they can do there. For instance, you can limit access rights to the ledger so that items (like cash payments that could be easily pocketed) can be added and edited, but not deleted.

7. Use your software's reporting capabilities. Many systems allow you to track activity for particular users. For example, you might run an audit report detailing what charges your facility manager has written off, or what cash payments front desk staff have deleted.

8. Internal audits are great, but make sure you conduct an outside audit every three years, recommends Arnold & Porter Kaye Scholer attorney **Alan Reider, JD, MPH**, who also spoke at Millennial Eye Live. In addition to flagging signs of embezzlement, outside audits can catch potential billing compliance problems as well.

Resource: To read the DOJ's statement, go to: https://www.justice.gov/usao-edva/pr/employee-indicted-embezzling-500000-medical-practice.