

How to prevent employee fraud

The best defense is a good offense, say these CPAs.

Feb 15, 2008

By: [Mark A. Master, CPA](#), [Sheldon H. Eveloff, CPA](#)

Medical Economics

Employee fraud can take many forms within a physician practice. But the accounts payable operation, because of the sheer volume of transactions, poses an especially big risk. If it isn't tightly controlled, someone intent on committing fraud can easily slip an improper vendor invoice or other fraudulent document through the cracks, thereby draining precious practice resources. Even an otherwise honest staff member may be tempted to float himself a "short-term loan" if he should fall on hard times.

To minimize these opportunities, you need to beef up the security of your accounts payable system. Establish well-thought-out internal control policies and practices, with checks and balances. Give each staff member a written job description, with a well-defined set of duties and a clear sense of how those duties fit into the overall system. Avoid having a single person handle the entire accounts payable operation; dividing up the duties makes it more difficult for any one individual to cheat. Finally, consider hiring an internal audit specialist to evaluate your internal controls, especially if your practice or practice environment has recently undergone significant change.

The policies and procedures you develop will help you safeguard practice assets, limit liability, and make your financial information system more reliable and accurate—provided you follow them. Here are some key fraud prevention measures you can start today.

Watch for unusual entries. The essence of double-entry accounting is that every transaction is two-sided, one action provoking an equal and opposite reaction. When a patient or third party pays a bill, your cash *increases* while your accounts receivable *decreases*. But what if a payment's offsetting entry is an employee loan account, exchange account, or inter-company account? In such cases, a warning bell should go off, signaling that the accounts payable entry may have been diverted by a member of your staff.

Validate purchases and expenses. Did you receive the product or service you were supposed to receive? Are the quantity, brand, and other specifications correct? A practice partner or office manager should always check, by comparing original vendor invoices, purchase orders, and receiving reports. All should be marked "paid," along with the check number. Investigate any transaction in which the same person authorized the purchase, approved the vendor invoice, and made the payment.

Be wary of "impatient" vendors. Legitimate vendors won't ask you to rush a payment, since

they understand your need to maintain internal procedures and controls. A vendor who pressures you to circumvent those controls may be in collusion with an employee set on misappropriating practice funds. Also, in larger practices, be wary of vendors who insist on dealing with the same accounting or administrative staff member or whose bills are always paid by the same person. If you suspect vendor-employee collusion, verify that the company has a valid business office, street address, and phone number.

Verify that your bills alone are being paid. If your accounts payable staff uses one checking account to pay a group of bills, it's not that hard for someone to slip in her personal telephone, utility, or credit card bill. Be alert to this possibility—and on the lookout for bills that include products or services delivered elsewhere.

Scrutinize canceled checks. Legitimate vendors deposit checks into their business accounts, so make it a habit to review both sides of canceled checks. A check that appears to have been cashed rather than deposited should raise alarms. So, too, should checks that have been deposited into personal rather than business accounts and checks bearing unfamiliar endorsements. A check payable to a vendor but endorsed by one of your employees, of course, is a sure sign of trouble.

Track vendor billing patterns. If you're used to receiving 12 invoices a year from Acme Company and you now have 14 or 15 payment entries, find out why. An unexplained jump in the number of payments could signal not only employee fraud but also related vendor kickbacks. If your billing records suggest that you may be paying two companies for the same service, investigate immediately.

Keep an eye on refunds. By examining vendors' monthly statements, you can gauge whether legitimate refunds are going back to the practice or being diverted to an employee's personal account. Patterns of overpayments to vendors should also raise red flags, since they offer yet another vehicle for accounts payable fraud.

Be alert to tax fraud. Fraudulent activity that gets the attention of the IRS can have devastating consequences for you and your practice. The attempt to cover up foul play by filing a bogus tax return, for example, can heap additional liabilities on your practice, especially if the culprit is a shareholder or managing officer. For this reason, extra vigilance is in order.

Adopt additional safeguards

Effective as these steps may be, there are a number of other things you can do to prevent the misappropriation of practice assets:

Review all bank and credit card statements. You, a practice manager, or a trusted partner should open the sealed statements and scrutinize them *before* they go to bookkeeping to be reconciled. Before paying credit card bills, insist on seeing the original receipts.

Monitor cash receipts and deposits. Someone who's *not* involved in making deposits or recording accounts receivable should open the mail, count the payments, and report payment totals to a partner or manager.

Reconcile accounts receivable/payable monthly, and require that all exceptions be cleared by a practice partner or manager.

Check out first-time vendors. Verify the supplier's name, address, and federal tax

identification number before placing an initial order.

Restrict authorization and access to finances. As part of this effort, password-protect computer files and set dollar limits on monetary authorizations.

Insist that employees take vacations. This is particularly true for anyone who works in accounting or another cash-handling function so you can double-check their work while they're out of the office. Employees who've been cross-trained can take over their functions, but you or a trusted colleague should take a look, too.

Watch for suspicious behavior. Be alert to signs of substance abuse, gambling, personal debt, or any other crisis or major lifestyle change among your employees, as well as indications of unusually high job dissatisfaction. If you notice any of these signs, monitor the employee's performance closely.

Conduct background checks on new hires. Check references and employment dates, and make sure time gaps are accounted for. Have employees with access to cash or other financial functions bonded. Obtaining a Fidelity Bond (available through your insurance broker) for high-risk employees with access to practice assets is an essential security measure.

For the fraud-conscious practice, having—and adhering to—strong internal controls is akin to practicing preventive medicine. Done properly, it's your best line of defense against all sorts of staff outbreaks of fraud.