

If you're going to make it, Make sure you keep it

As a CPA and healthcare consultant, one of the things that continues to concern me is employee theft within a medical practice (or any other healthcare entity for that matter). You trust your staff, right? You know them to be loyal and dedicated individuals who would never steal from the practice, right? Unfortunately physician practices are no less at risk of employee theft than any other business.

In fact, physician practices may be particularly vulnerable to theft, especially since doctors concentrate on treating patients and delegate the running of the office to others. As a result, I see that a lot of physicians aren't as vigilant about keeping a personal eye on things as some other business owners. So it's imperative for your practice to implement the proper safeguards and internal controls to prevent theft. Here are a few simple precautions to adopt in your office:

Heed red flags from the get-go. The best way to prevent theft is to hire the right people. Also do situational interviewing by giving a candidate good scenario questions where you can create a scenario and see how they would handle a situation. For example, ask the candidate how he or she feels about delegating tasks to other staff members. Things that you would want to look out for are people who want to do everything and handle everything. If the candidate tells you in the interview, " 'I handle all of the revenue cycle. I went to the bank every day. I did this. I did that.' You want to stay away from people who are keepers of all the keys."

Conduct background checks. Background checks are another essential part of the interview process but believe it or not there are many medical practices that don't do this on a regular basis. You can be so easily fooled in an interview, so check applicants' criminal history, do a Google search of their name, and look into their credit history to see whether they're under financial strain. If they have really bad credit history, don't hire them if they're going to be handling money. Background checks are fairly inexpensive but no matter what the final price, the costs are well worth the time and money you could save both yourself and your practice in the future.

Crosstrain employees. If you've already hired an employee, watch out for other warning signs, such as an employee who never takes a day off or uses vacation time (I'm a big believer in mandatory vacation leave – employees must take at least one week of their vacation in consecutive days.) If an employee thinks he or she can't leave because nobody else can do his or her job, you've got problems. Either that person is stealing from you, or you don't have enough people trained to handle several different tasks and instructions.

One way to avoid such a dilemma is to crosstrain employees. In smaller practices, physicians often place the most responsible person in charge of every aspect of billing. However, if you have the same person opening the mail, making the bank deposits, and posting payments to the billing system, you may be asking for trouble (Which is why you need a lockbox arrangement with your bank!)

Ideally, each aspect of the billing process should be assigned to a separate employee. If you have one person doing it all, add at least one other person to the process. The change can be as simple as asking a receptionist or medical-records clerk to open the mail and keep track of the checks that come into the office. That way, it doesn't leave you dependent on one person-that's the biggest thing.

Pay attention. Unusual employee behavior is not the only tip-off that embezzlement may be occurring in your practice. Irregularities in audits and inconsistencies in monthly reports should also raise red flags (Do you have a monthly practice management reporting system in place?). However one simple prevention idea is to establish a control system for your charge tickets. Make sure all charge tickets prenumbered (or assigned a number by the computer) and accounted for at the end of the day. Print and review the “missing ticket report” every day and crosscheck your charge tickets against your schedule for the day.

If you saw 20 patients, you should have 20 charge tickets accounted for. Otherwise, an employee could throw a ticket away and collect the payment instead of posting it. Through just plain error, you could lose money if you don't control your charge tickets.

Also, make sure each day's payment posting activity is closed and reconciled to the deposit slip (You must make deposits daily!). One sure red flag is when posted receipts in the medical billing system is more than the money that actually went in to your bank account.

It's also a good idea to audit your accounts payable as well and make sure your invoices match up with the checks that you're sending out. People can steal through the accounts payable process just as easily as within the accounts receivable process.

Bond your employees. If embezzlement were to take place in your practice, an employee dishonesty bond reimburses you for the amount stolen. Not purchasing such a bond could cost you your practice. I know of one instance where a physician discovered that his office manager had been embezzling from him for 10 years straight - She had been doing it since day one. Although the former employee had to pay restitution to the physician, he never really recouped what he lost. He nearly went bankrupt because of it. What it all boils down to in the end is that it's better to be safe than sorry.

Stay involved in the financial side of your practice

To defend against fraud, physicians must get involved in the day-to-day operations of the office, at least in a limited way. To protect yourself, put the following financial controls in place:

Sign all your checks yourself. Keep the office manager off the signature card and don't use a signature stamp. Don't sign a check unless there's an original invoice that's been marked "paid" so that it can't be paid a second time—either accidentally or deliberately. Check to make sure the invoice amount seems reasonable. For example, if you usually spend \$200 per month on office supplies and suddenly you have an invoice for \$1,000, question that. Be on the lookout for new suppliers, too.

Open bank statements yourself. You may not have time to reconcile the bank statement every month, but at the very least, you should be the one to open the envelope. Scan the bank statement and look to see that the ins and outs of what's happened in that month seem right to you. Look through all the canceled checks. Does it look like your signature? Does it look like the payees are people you would expect to have paid?

Okay all changes to payroll. Ideally, doctors should be the only people in the practice with the authority to add an employee to the payroll or change wage amounts. If it's necessary to allow an employee to change the rates, make sure your payroll company issues a report of the change directly to you. Also, make sure you review all overtime. It's very easy to steal by padding hours.

Require written annual competitive bids from your vendors. Unless you get bids for products that you use in volume, you could be overpaying. Requiring written bids prevents employees from entering into fraudulent, long-term partnerships with a vendor. I know of a case in which a practice employee paired up with a member of the vendor's finance staff to overcharge the physician and split the profits.

If you would like a free internal control checklist/work program, email me at reedt@rtacpa.com and I'll be happy to send it to you. As the only saying goes, "an ounce of prevention is worth a pound a cure."

Reed Tinsley, CPA is a Houston-based CPA, Certified Valuation Analyst, and healthcare consultant. He works closely with physicians, medical groups, and other healthcare entities with managed care contracting issues, operational/financial management, strategic planning, and growth strategies. His entire practice is concentrated in the health care industry. Please visit www.rtacpa.com