

BY MARILYN HADDRILL

# Taking Care of Business

*Employee fraud is more common than you think, and medical practices are especially vulnerable if the physician doesn't keep an eye on the books. What you need to know to protect your practice.*



ILLUSTRATION ©2003 CLAIRE FRASER

---

**O**NE NEW MEXICO SURGEON WAS TOO hurried to question why his receptionist seemed to pick an inopportune time, such as when he was rushing out the door on an emergency, to insist he sign checks for office utility bills.

“Didn’t we just pay this a few weeks ago?” he would ask.

His receptionist joked about how time flies. But one day the physician’s bookkeeper at an accounting firm happened to notice two sets of electric, water, and sanitation bills. Because the physician operated from only one location, multiple bills made no sense.

The surgeon was notified. After a meticulous review of

records, his accountant discovered that the surgeon had been signing checks paying for the receptionist’s home utility bills.

“The receptionist had been there six to seven years prior to starting this behavior,” says Las Cruces, New Mexico, CPA Don Beasley. “We looked at the records and found no evidence that this had happened before. But what we did notice was a change in a life situation for that person. She had gotten a divorce about six months before and was starting to have some financial problems.”

Beasley says most physicians likely will encounter at least one incident of employee embezzlement or fraud over several decades of running a practice. In his office, accountants handle physician office fraud at least once or twice yearly in amounts ranging from \$1,000 to \$130,000. A long-time employee in these cases might betray both friendship and trust by altering records or engaging in other scams to hide evidence of embezzlement that could span months or even years.

“A lot of times, the patient will owe money at the time of the visit through a co-pay-

*Continued*

### Signs of Trouble

While you should of course avoid paranoia, be aware that some factors might signal a problem. These include:

- ✘ *An employee whose life circumstances suddenly change—i.e., a divorce causing financial hardship or the sudden adoption of lavish spending habits, such as purchases of expensive new cars or clothes.*
- ✘ *Revenues that inexplicably seem to be declining, especially when the physician has a full case load.*
- ✘ *A “loyal” employee who refuses to take time off, which prevents a substitute from handling financial transactions or discovering suspicious or altered records. A dishonest employee might insist on being in charge of all aspects of daily office procedure while refusing to share duties with co-workers.*

---

## EMPLOYEE FRAUD

*Continued from previous page*

ment system required by the insurance company,” Beasley says. “We had one situation last year where the receptionist took care of all the postings and patient receipts. The receptionist then was pocketing all the co-payments and making adjustments on the ledger for each patient to eliminate all evidence of that charge.”

Don't put your eggs in one basket

Beasley says it's essential that duties be divided so that no one employee manages all aspects of a financial transaction. Questions new physicians should ask themselves as they set up internal controls are:

- How do we handle receipts?
- Who is in charge of receipts?
- How do we balance our accounts each day?

“Don't assume that a group practice you are joining already has all the internal controls in place that it should, either,” Beasley says. “Weaknesses may exist within the system. It's not that anyone is necessarily doing anything illegal or wrong. But many times a practice grows from a doctor, a nurse, and a receptionist. The same old procedures are still in place, even though there are now more employees.”

A [Federal Bureau of Investigation](#) analysis of white collar crime from 1997 through 1999 indicated that most of offenses involved counterfeiting or forgery. Of 5.9 million economic offenses analyzed, almost 37,000 took place in medical environments—pharmacies, doctors' offices, or hospitals. Of these cases, 338 involved embezzlement.

[The Association of Certified Fraud Examiners](#) concluded after an extensive study and update in 2002 that small organizations (100 or fewer employees) suffer the most per capita incidents of

fraud (\$127,500 median loss) because sophisticated internal controls were apt to be missing in these more informal occupational environments.

The association also estimates that occupational fraud, defined as misuse of employer assets, causes losses of 6 percent of total revenues. Based on the gross domestic product of 2002, this would amount to \$600 billion, or \$4,500 per employee. Experts say physician office fraud schemes range from bogus charges made to insurance companies to cash payments stolen from patients.

In Palm Harbor, Florida, ophthalmologist Lyda Tymiak, says an associate in her practice detected employee embezzlement after patient charges were altered on encounter forms. The associate would fill out the form with the proper amount owed, and the patient would pay, sometimes in cash. The employee handling the transaction then would fill out a different encounter form reflecting a lower amount. The difference was pocketed.

“At the time, encounter forms were not consistently numbered,” Tymiak says. “After that, every encounter form was numbered so there was no way of switching. Unfortunately, when there is one episode of dishonesty, there very likely are even more. Cash especially is very, very tempting.”

Because of the incident, Tymiak says she developed a daily transaction log enabling her to review numbers of patients seen, encounter forms, appointment cancellations, payments, and form of payment (cash, check, or credit card).

“Just the fact that you are looking tends to help,” Tymiak says. “You don't have to examine every little thing. But if employees know that you are taking an

interest, they are more careful. I also plan to start reviewing our system to make sure the person who opens the checks is not the same person who posts the checks, because that's another area where there are major temptations.”

Tymiak says bank statements should be reviewed by a person other than the one who opens them, preferably, either the physician or an accountant.

“You can't re-do every task,” Tymiak says. “But you do have to have safety checks. I now have a person outside my office, a bookkeeper, who writes and reconciles my checks. This is an added layer of oversight. Physicians tend to be very busy, and not necessarily business-oriented. And they are trusting. Employees become like family. You get involved in the medical part of the practice. You think things are running well and properly. Yet, someone can be stealing right from under your nose.”

A matter of trust

In Iowa, Alicia Tullo, RN, handled business dealings for her husband, Ralph Tullo, MD. The two since have moved to Heathrow, Florida, and are setting up a Breast Health Institute in Orlando. But when Tullo previously worked for a hospital-based radiology group in Iowa, Mrs. Tullo says they encountered embezzlement from the very first employee she ever hired.

“I hired her because she was smart, she was teachable, and because she was a single mom,” Mrs. Tullo says. “I wanted to give this girl a chance. I eventually had a billing company, but I started off billing only for my husband, who was the director of a radiology department. Between this employee and myself, we did the job. Eventually, my business grew to seven employees. This

## EMPLOYEE FRAUD

Continued from previous page

### Protecting your practice

*Internal fraud in all business areas continues to increase at a cost of billions of dollars annually, says Jim Harris, a senior vice president and manager of professional banking services at Wells Fargo Bank in El Paso, Texas.*

**In the El Paso County Medical Society journal, Harris advised physicians to protect their practices by using some of these safeguards:**

- ✚ Open a separate banking account for your payroll or use a payroll service. This blocks employee access to operating accounts and information. Also consider direct deposits of funds to employee accounts to reduce possibility of paycheck fraud.
- ✚ Encourage patients to pay with credit cards, which means payments can be electronically deposited into your bank account the next day. This reduces the chance of payments being misdirected.
- ✚ Consider a lock box service in which your receivable checks are sent directly to the bank instead of to the office. This way, you receive a daily copy of checks received along with a tally of daily deposits (usually lock box services are more appropriate for larger practices due to fees).
- ✚ Keep bank account checks and deposit slips in secure locations. Make sure computers are turned off and locked up after hours.
- ✚ Keep sensitive information such as personal credit card statements out of sight. When you no longer need paper records, shred them.
- ✚ Pay special attention to checks cashed out of sequence or unfamiliar check numbers. Also watch for unusually large numbers of checks made out to "cash."
- ✚ Watch for unusual fluctuations in your bank account activity, such as lower balances, smaller deposits, or unexpected expenses.
- ✚ Consider insurance coverage protecting your practice if employee fraud or embezzlement were to occur. ■

girl who was with me from the very beginning turned out to be the one who was doing the embezzling. She worked for me about four years."

After growing suspicious and tracking through the records, Mrs. Tullo discovered the employee had used various methods to steal what were at first small amounts. But as time passed, the employee became greedier. Thefts of

cash payments were hidden, for example, through methods such as falsely recording debts as being written off.

"This girl was able to embezzle because I trusted her. That was my mistake," Mrs. Tullo says. "Because she had worked so many years for me, I allowed her to handle refunds. Before, I was the only person who could handle refunds. If the refund was legitimate, I

would issue a check and then sign it. When my husband and I went on a four-week vacation, this girl went berserk. She refunded many bogus accounts, and the money went to her for things like car payments and a wedding gown."

When the total embezzlement of about \$30,000 was documented, Mrs. Tullo says she and her husband then were faced with the agonizing choice of whether or not to pursue prosecution.

"When I discovered this, it really broke my heart," Mrs. Tullo says. "I cried because I was so disappointed in her. I nurtured her. I gave her a skill she had never before had. For her to turn around and do this to me was very, very hurtful. When the county prosecutor asked if I would be willing to prosecute her, I asked him: 'Would you do it if you were in my place?'"

She says the prosecutor didn't hesitate to answer: "Definitely."

She learned from the prosecutor that employee theft in physician practices is extremely common, and is, in

### Set up internal controls

- ✓ While financial aspects of your practice might seem tedious, accept that you must involve yourself in oversight to minimize chances of employee theft. Even if you join an existing practice, make sure you ask appropriate questions about how postings, receipts, and deposits are handled.
- ✓ Maintain checks and balances by trying never to have one employee in charge of all aspects of the practice's finances. Separate tasks such as posting charges, preparing refund checks, or reconciling bank statements. If you do have a small practice with only one employee, make sure you require daily summaries of patient visits, billings, and income received from insurance companies and other payers. At random intervals, compare a day's transactions with corresponding bank records.
- ✓ Make sure you also follow the rules. Any employee who sees you take cash without reporting it on your income tax, for example will imitate the standards you set. A dishonest employee caught stealing from the practice could in turn threaten to report irregularities to the Internal Revenue Service or regulatory agencies. Honesty is the best policy where ALL parties are concerned. ■

---

## EMPLOYEE FRAUD

*Continued from previous page*

fact, committed in virtually every practice at some point. Yet, many times, a physician does not pursue criminal charges against the offender. This makes the problem even worse because there are no consequences for criminal behavior.

"This is a very, very common crime," Mrs. Tullo says. "But the most common complaint from physicians is that they feel they don't have the time to deal with it. Or they say: 'I only lost \$20,000 so I'll just fire the person.' They don't want to look stupid. They don't want to be in the papers. They don't want anyone talking about their practice. They come up with all kinds of reasons not to press charges."

She says the prosecutor convinced her to proceed with charges when he explained what happens when crimes go unpunished: "If they do it to you, then the chances are they've done it before and they will do it again."

Sure enough, after filing charges and sending the employee to jail, Mrs. Tullo says she discovered the woman had a record of past thefts including stealing from a women's clothing store where she had worked previously. Ms. Tullo says the experience also taught her to check employee references and background thoroughly before hiring. Mrs. Tullo became an expert at setting up internal billing procedures, and later began consulting for other physician practices.

But not all prosecutors seem that willing to deal with white collar crime even when a physician is willing to press charges, according to Robert Berry, MD, who operates a primary care clinic in Greeneville, Tennessee. He says he has ample evidence that an employee embezzled from him for 16 months from 2000 to 2002. Even

though documentation includes canceled checks she wrote to herself, Berry says he has been unable to persuade local officials to prosecute. The woman since has moved outside the jurisdiction.

"I have a different type of practice from most physicians who end up being salaried or having someone else take care of business aspects after they are hired on," Berry says. "I don't take any third party payments, so it should be very easy to make sure there is no embezzlement. I just trusted her, that's all. That's why I hired her. She seemed like a trustworthy person."

Berry says the woman used his corporate checking account and signature stamp for unauthorized purposes such as paying off personal credit card debts. He estimates the check forgeries cost him about \$60,000.

"Something like that really can't happen today," Berry says. "I have one office person. That's it. She takes the cash or credit card payments. We have a patient log. If we see 20 patients a day, she logs all that in, including how much we have received. Then she brings out the cash box. I count out the cash, and put aside a certain amount (for change) for the next day. Every day, this is reconciled. Right after the last patient leaves, I lock the door. And then I make the deposit. There's really no way in this type of practice that I can have embezzlement now."

### The fraud triangle

Three separate elements must come together for employee fraud to occur, says Jerry Bartram, CPA, of Redlands, California. Those elements are motive, opportunity, and rationalization. Though not a certified fraud investigator himself, he belongs to the

Association of Certified Fraud Examiners that has defined the "triangle" of factors leading to fraud.

"It's like a 'fire triangle,'" Bartram says. "In fire fighting, you learn that if you have an air source, and then you have heat, and you have fuel, then you automatically have fire."

Bartram, also a member of the [Healthcare Finance Management Association](#) and [Society of Medical-Dental Management Consultants](#), says medical practices are particularly susceptible to employee rationalization.

"He's not paying me overtime. She's not treating me fairly. I work harder than anyone else in the office works, and yet I don't get recognition or pay increases. There are a lot of things that go through a person's mind," Bartram says.

Giving the person an opportunity to take the money through means such as inadequate internal controls also adds to the equation.

"But motive is where fraud really kicks in," Bartram says. "It might involve something the employee is trying to cover up that she doesn't want a spouse to know about. Or maybe a tragedy has occurred in the employee's life."

Bartram described one classic case he investigated where a long-time, trusted controller at a Christian university learned that his wife had terminal cancer.

"He ran out of insurance benefits," Bartram says. "He was watching his wife die, and he couldn't stand it. He started kiting checks (exchanging checks between two or more bank accounts to create the impression a balance exists that really isn't there). Pretty soon he was in head over heels. The unfortunate part is that his wife died anyway, and he wound up in disgrace. For a long time, he was never

---

## EMPLOYEE FRAUD

*Continued from previous page*

motivated. But his rationalization was: 'My wife is dying. They should have had better benefits for me. They didn't, and I had a right to the money.'"

A startling statistic compiled by fraud investigators reveals that older embezzlers hit employers harder in the pocketbook. A median loss of \$18,000 is associated with embezzlers aged 25 or younger. A median loss of \$500,000 is associated with embezzlers 60 or older.

"The reason is that you trust a person who has worked for you for years more than anyone who has just started working for you," Bartram says. "And also an older person generally has greater access to assets. The 60-plus crowd will have fewer incidents, but much larger amounts. That is what really gets physicians and anybody who is in the trust business—to find out that someone who has been a faithful worker all their lives has been stealing them blind." ■

*Marilyn Haddrill lives in Las Cruces, New Mexico. This is her first article for Unique Opportunities.*