Carolyn L. Hartwell, PhD, CPA, Susan S. Lightle, PhD, CPA (inactive), Randall K. Domigan, CPA, CFE

Is Your Practice at Risk for FRAUD?

Without reasonable controls, you may be inviting embezzlement.

The newspaper headline read, "Office Assistant Indicted on $350,000 Embezzlement Charge." The six-physician suburban office was shocked by the revelation. Sharon, a 60-year-old grandmother of two, was active in her church and frequently socialized with co-workers. Early one Monday morning after returning from vacation, she was met by law enforcement officials and subsequently arrested. The officials found approximately $100,000 in checks from insurance companies and patients in her purse at the time of the arrest. As often happens, her co-workers and physician employers were caught completely off guard. Sharon had been a trusted employee for five years. (For an inside look at her embezzlement, see "How did Sharon do it?" at the right.)

How can you be sure your office is not at risk for a similar fraud? This article will provide an overview of accounting controls that are designed to reduce that risk.

Occupational fraud

In a 2010 report, the Association of Certified Fraud Examiners (ACFE) summarized the results of a study of 1,843 cases of occupational fraud investigated between January 2008 and December 2009.[1] They found that businesses with fewer than 100 employees accounted for the highest number of fraud cases in their study (31 percent), with a median loss per case of $155,000. The health care industry ranked fifth in number of cases with 107 (5.9 percent) and a median loss of $150,000. See page 24 for a summary of the most common types of fraud in health care.

A reason identified by the ACFE for the disproportionate losses to small businesses is that they typically have limited fiscal and human resources available to fight fraud and, in part as a result, they have poor internal controls. While they may not be able to *prevent* fraudulent activity, basic internal controls provide a safety net that proactively detects a small misappropriation before it snowballs into a $350,000 fraud like Sharon's. Physicians, like many small business owners, may believe that they don't need internal controls because they have a small group of trusted employees. Their tendency to focus on patient care rather than back-office operations may also leave them vulnerable to embezzlement.

KEITH NEGLEY

Common weaknesses in medical practices

Failing to properly separate accounting functions, particularly those dealing with cash, is common among medical practices. For example, some practices allow the person who opens the mail to post the payments received in the accounting system. That same person may also be allowed to make accounts receivable adjustments (such as patient or insurance write-offs) in the system. This situation gives the employee the opportunity to steal payments and write off any balance due. Questions are unlikely to arise concerning accounts with zero balances, so the fraud may go undetected for an extended period. It is imperative that the person who opens the mail and has access to cash not be the person who records it in the accounting system. If these job functions are separate, two or more employees would have to collude for the theft to be concealed.

Another common weakness is permitting the accounts payable clerk to approve new vendors, approve invoices to be paid or even sign checks. This gives the employee the opportunity to authorize and make a payment to a related party or even a fictitious business from which he or she can benefit. One business was surprised to find that an accounts payable employee had approved and paid fictitious bills for uniform cleaning week after week. The cleaning company was nonexistent, and the payments were deposited into a bank account the employee had created. If the authorization, verification and payment duties had been separated, this fraud would not have been possible.

Many practices have implemented electronic banking, including automated clearinghouse (ACH) transactions and wire transfers. Some practice owners may not even be aware that their business is using electronic banking because it was initiated by office personnel and the practice's bank offers the service for free. Electronic banking can increase efficiency and cut down on paperwork, but practices should be aware of its risks. Controls should be in place to prevent an unauthorized individual from initiating electronic payments out of the bank account, in much the same way as requiring that only physician partners may sign checks. If a practice allows non-owners both to sign paper checks and to initiate electronic transfers, the opportunity for fraud increases.

Controlling fraud

The key to controlling the risk of fraud is to understand why fraud happens. Generally speaking, three factors are present when fraud is committed: incentive or pressure to commit fraud, the ability to rationalize or justify the fraudulent behavior, and perceived opportunity to get

HOW DID SHARON DO IT?

Sharon was responsible for billing, including processing insurance payments and handling write-offs. Most insurance checks were direct-deposited, and only the explanations of benefits (EOBs) were sent to the office for processing. Payments from patients either received by mail or collected in person were handled by the front-desk employees, who were responsible for making a list of the checks, totaling the cash and preparing a deposit slip. A copy of the deposit slip was given to the office manager.

The list of checks was given to Sharon to update the patient accounts. Responsibility for taking deposits to the bank was shared by three people, including Sharon. Sharon frequently volunteered to relieve the others of this duty. The office policy was to open all mail and deposit all cash receipts at the end of the day. However, if they were particularly busy, mail was sometimes set aside to be opened the next day.

The fraud was relatively simple. Sharon arrived early one day and took a piece of unopened mail that contained a patient's check for $123. She hid it in her desk and at the end of the day prepared a new deposit slip, adding the $123 check and decreasing the *cash* total so that the total deposit amount was unchanged. She pocketed the cash and made the deposit.

As an experienced billing clerk, Sharon knew that if she didn't adjust the patient's account for the amount taken, the patient would eventually complain and the theft would be detected. Since Sharon regularly recorded contractual insurance write-offs, it was easy for her to increase the write-off of a given patient's account by the amount she had stolen. The patient's balance due would now be correct, and patient totals would agree with the accounts receivable on the books. On the other hand, revenues were understated, affecting cash flow and bonuses – but in an environment of declining Medicare and insurance reimbursements, reduced revenue did not seem unusual. Since no one seemed to notice, she did it again.

Although the office manager had copies of the deposit slip prepared by the front-desk employees, she did not receive a copy of the actual deposit slip processed by the bank. Since the totals of the deposits were the same, the fraud was not detected by the office manager. This could have gone on forever if not for the curiosity of a suspicious co-worker. Not knowing exactly what was going on, the co-worker asked a friend who worked at the bank to send her a copy of a recent deposit slip. When she received it, she gave it to the office manager, who noted an unusual cash deposit of 15 cents. She immediately went to the managing partner's office and said, "We have a problem."

INTERNAL CONTROL AND FRAUD PREVENTION CHECKLIST

Answer each question with a Y for Yes, N for No or DK for Don't Know. If you have a significant number of "no" and "don't know" responses, consider whether a more formal review is warranted.

CASH RECEIPTS AND ACCOUNTS RECEIVABLE	
Y N DK	Does the practice use a lockbox, or are the majority of deposits transmitted electronically to the practice's bank account?
Y N DK	Do different people open the checks from the mail, make out the deposit slip, make the deposit and post the deposit to your receivable ledger?
Y N DK	Are restricted endorsements placed on checks upon receipt (e.g., "For Deposit Only")?
Y N DK	Does someone compare the posting of the customer accounts to the cash receipts?
Y N DK	Are cash receipts deposited promptly and stored in a secure location until they are deposited?
Y N DK	Are pre-numbered receipts used for actual cash receipts?
Y N DK	Does an individual without accounts receivable duties do collection calls for the practice?
Y N DK	Are there authorization procedures in place for writing off uncollectible accounts, and is that handled by someone other than the accounts receivable clerk?
Y N DK	Are actual cash receipts compared to budgets, and are variations investigated?
Y N DK	Are system-generated accounts receivable reports (accounts receivable aging schedules) examined and compared to the general ledger?

CASH DISBURSEMENTS AND ACCOUNTS PAYABLE	
Y N DK	Are all disbursements made by check except for minor petty cash disbursements?
Y N DK	Is the person signing the check someone other than the initiator of the check or the accounts payable staff?
Y N DK	Are payables properly approved?
Y N DK	Is a second signature required for checks over a pre-determined dollar amount?
Y N DK	Are blank checks stored in a secure location?
Y N DK	If signature stamps are used, are they used only by the individual whose signature is on the stamp?
Y N DK	Are bank statements opened and reviewed periodically by an owner or someone outside of accounting before they are given to accounting to reconcile, or are disbursements clearing the bank periodically reviewed online?
Y N DK	Are vendor lists periodically reviewed by owners or upper management?
Y N DK	Is Positive Pay (a treasury function offered by most financial institutions) used by the practice?
Y N DK	Are there controls in place for the use of practice credit cards?
Y N DK	Are actual expenses compared to budgets, and are variations investigated?
Y N DK	Are system-generated accounts payable reports such as accounts payable aging schedules examined and compared to the general ledger?

ONLINE BANKING/AUTOMATED CLEARINGHOUSE (ACH) TRANSACTIONS AND WIRE TRANSFERS	
Y N DK	Does your agreement with the bank require involvement of a practice owner to enable ACH debits, credits and wire transfers?
Y N DK	Are daily transaction limits set up for ACH payments?
Y N DK	Does the practice's ACH system require more than one person in the process to make a payment?
Y N DK	Do individuals at the appropriate level in the practice have access to the online banking function?
Y N DK	Are the controls or safeguards that are in place through your bank for ACH transactions and wire transfers documented and reviewed on occasion to determine the ongoing appropriateness of the controls?

PAYROLL	
Y N DK	Are pay rates of employees reviewed regularly by owners or upper management to determine the accuracy?
Y N DK	Are employee payroll records reviewed by owners or upper management to determine whether there are any fictitious employees and to confirm that time charged by hourly employees is reasonable?
Y N DK	Is an outside payroll service provider used?
Y N DK	Are any self-directed employee savings plans periodically reviewed to determine that the withholding from the employee matches the contribution going into the employee's self-directed account?

Y	N	DK	Is there a proper system in place for authorizing pay rate changes and adding new employees into the payroll system?
Y	N	DK	Are there procedures in place to ensure payroll tax liabilities and 401(k) withholdings are paid on time?
			GENERAL CONTROLS
Y	N	DK	Are vacations for the individuals in your accounting department required, and does someone else do their job while they are gone?
Y	N	DK	Are all employees who handle cash receipts and disbursements bonded, or do you have adequate insurance coverage for employee misconduct?
Y	N	DK	Are only authorized individuals given access to the accounting system and general ledger, and are appropriate user names and passwords used?
Y	N	DK	Do practice personnel know that owners and upper management take an active role in reviewing financial data and transactions?
Y	N	DK	Are bank accounts reconciled regularly by someone without cash receipt and disbursement duties?
Y	N	DK	Do you have a mechanism in place for employees to report suspected fraud anonymously?
Y	N	DK	Do you provide ethics and fraud-awareness training to all employees?

away with it. These factors are sometimes collectively referred to as the fraud triangle.

Incentive or pressure to commit fraud. In the current economic climate, the risk of occupational fraud may be greater than in better times. An employee whose spouse lost his job may consider "borrowing" a small amount to make a mortgage payment with the intent of paying it back as soon as possible. But when the employee is short again next month and realizes how easy it was to get away with the first misappropriation, the temptation to repeat the offense may be irresistible, and so the snowball begins to grow. To some extent, good hiring practices can reduce the likelihood of having an employee with an incentive to commit fraud. Thorough background checks – to screen applicants with a history of financial problems or behaviors such as gambling and drug use that can lead to financial problems – may reduce this risk. However, any employee's circumstances can change over time, putting pressure on that person to do something he or she ordinarily would not do. Although such life changes may be out of the employer's control, it is wise to watch for signs of problems and if they arise consider reassigning the employee to a position that does not have access to cash.

The ability to rationalize or justify the fraudulent behavior. Rationalizing bad behavior is a basic human tendency, particularly among disgruntled employees or those who feel they have been treated unfairly. By being alert to employees' concerns and addressing problems proactively, physicians may be able to reduce the likelihood that an employee will rationalize committing fraud as a way of "evening the score."

Perceived opportunity to get away with it. Appropriate policies and procedures, rigorously enforced, will effectively deter most attempts at fraud. Furthermore, a reasonable system of checks and balances will detect an initial attempt before it escalates. Creating a strong control environment starts with the tone at the top of the organization. The physician partners should communicate by word and example that controls are important and that failure to follow them will result in negative consequences. An anonymous employee "hot line" or locked message box for communicating suspected fraud or violations of policies and procedures is a good way to send that message. Alternatively, employees could be instructed to report suspected problems to a designated physician. In the ACFE

Medical practices, like other small businesses, are at particular risk of fraud because of their often lax internal controls.

Many practices fail to separate accounting functions that, if performed by one person, facilitate undetected fraud.

About the Authors

Carolyn L. Hartwell is associate professor of accountancy and Susan S. Lightle is professor of accountancy, Wright State University, Dayton, Ohio. Randall K. Domigan is a manager with Brady Ware in Dayton, Ohio. Author disclosure: no relevant financial affiliations disclosed.

Article Web Address: http://www.aafp.org/fpm/2011/1100/p20.html

study, 40 percent of the fraud cases were initially detected through a tip (more than any other means of detection), and 49 percent of those tips were reported by employees.

Training office personnel in fraud awareness and ethics can be a relatively inexpensive way to strengthen the control environment and make a fraud hot line more effective. Practice owners sometimes have a false sense of security because they engage a CPA to perform payroll and tax services. However, these services do not include a review of internal controls. An internal control review by a consultant or CPA firm with experience in medical practices and fraud prevention can identify areas of weakness and provide recommendations for improvements. Once the recommendations have been implemented, periodic "check-ups" (every three to five years and after any significant change in the accounting system) will maintain effective controls and deter fraud.

A strong control environment must be coupled with sound internal control policies and procedures to effectively deter fraud. See the "Internal control and fraud prevention checklist," page 22, for recommended policies and procedures for cash transactions. A key concept underlying these recommendations is segregation of duties. As you can see from "How did Sharon do it?" (page 21), these controls were not in place in the practice that employed her.

However well designed, strong internal controls cannot guarantee that fraud will not occur, so an important part of fraud risk management is having adequate insurance. Bonding employees who handle cash and including insurance coverage for employee misconduct can minimize losses if fraud occurs. It is also important to review insurance policies to be sure that the amount of coverage is reasonable. Insurance covered less than one-third of the loss for the medical practice described earlier.

Fraud tends to occur where someone has the incentive to commit fraud, the ability to rationalize it and a perceived opportunity to get away with it.

A fraud-prevention checklist can help you determine your practice's degree of risk.

Nothing can prevent fraud absolutely, so having adequate insurance is an important part of fraud risk management.

The take-home message

No matter how trustworthy you think your employees are or how long they have worked for you, your accounting system should include appropriate controls to mitigate the risk of fraud. While implementation of these controls may require some initial cost in terms of redefining processes and in terms of owner oversight, the benefit of managing the risk of fraud far outweighs the cost.

A simple checklist like the one on page 22 is a good starting point for determining your exposure to occupational fraud risk. Although there is no formula to quantify each practice's fraud risk based on responses to the checklist, if you have a significant number of "no" and "don't know" responses, we suggest that you discuss them with a professional experienced with medical practices and fraud prevention to determine whether a more formal internal control review is warranted. FPM

Send comments to **fpmedit@aafp.org.**

1. Association of Certified Fraud Examiners. Report to the Nations on Occupational Fraud and Abuse: 2010 Global Fraud Study. http://www.acfe.com/rttn.aspx. Accessed Oct. 18, 2011.

MOST COMMONLY REPORTED FRAUD SCHEMES IN HEALTH CARE

Type of fraud	Description	% of cases
Corruption	Use of influence in business transactions in a way that violates a duty to one's employer in order to obtain a benefit to oneself or others	29%
Skimming	Theft of cash before it is recorded on the organization's books	22.4%
Billing	Causing the organization to issue a payment by submitting invoices for fictitious goods or services	21.5%
Non-cash misappropriation	Theft or misuse of non-cash assets of the organization	19.6%
Check tampering	Forging or altering a check on the organization's account or stealing a check legitimately issued to another payee	12.1%

Note: Some cases involved more than one type of fraud. Source: Association of Certified Fraud Examiners. Report to the Nations on Occupational Fraud and Abuse: 2010 Global Fraud Study. http://www.acfe.com/rttn.aspx. Accessed Oct. 18, 2011.