Preventing Fraud in Medical Practices

Executive summary

The shift of financial responsibility for healthcare costs from employers and insurers to patients poses many new challenges for medical practices. It means learning how to collect cash from patients and then understanding how to manage that cash so it doesn’t end up in the wrong hands.

Contents

Mind human resources. .... 2
Create policies ............ 3
Stop signature stamps .... 3
Manage financial records .. 3
Control cash ............... 4
Deploy automation ......... 5
Establish a lockbox ....... 6
Watch account adjustments ........ 6
Experts estimate that 5% of business revenues are lost to fraud, a loss that no medical practice can afford. Identity theft is on the rise as more financial transactions take place online, and individuals are conjuring up new schemes that target medical practices. However, another enemy may be within. Much fraud is committed by someone who works for the organization experiencing the loss. Fortunately, there are a number of controls and strategies that medical practices can take to prevent both external and internal fraud.

According to the criminologist Donald Cressey, the environment becomes ripe for fraud when three factors converge: opportunity, motivation and rationalization. These three pressures, collectively known as the “fraud triangle,” are certainly present in many medical practices.

Opportunity for fraud abounds in medical practices because they tend to hire employees at low wages and then put them into high-stress jobs with the responsibility to collect and process cash payments. Making matters worse, the rapid increase of patient financial responsibility means these employees handle considerable sums in the form of copayments, coinsurance, unmet deductibles, balances and deposits with what is often only cursory oversight. Add in the extent of personal data about patients to which these workers have unfettered access, and the lax cash controls and unsophisticated management systems typical of many medical practices, and the climate is perfect for fraud. Unfortunately, this scenario is all too true in many medical practices. (See the sidebar on page 3 for true stories of recent fraud experienced by medical practices.)

The best medicine for fraud — internal or external — is prevention. The attack on fraud should include careful screening of employees and improving internal systems to better monitor cash collections and funds management.

**Mind human resources**

During the hiring process, conduct thorough reference checks. Be aware that references can be falsified — sometimes by an accomplice posing as a previous employer — and that resumes can be misleading. According to numerous research studies, more than half of all job applications contained inaccurate information and nearly half of all resumes are fabricated. In this era of time-of-service payments, look into the backgrounds of all staff considered for hire, not just managers or those who will be involved in accounting.

Fraud prevention doesn’t end with the hiring process. Be cognizant of employees who refuse to take vacation or start working odd hours when others are not around. Question an employee who becomes edgy about sharing his or her job responsibilities. Keep an eye out for employees who have documents, statements or other records of the practice that aren’t in their normal line of work, such as a front desk clerk who has a copy of the medical practice’s banking statement.

Most physicians who have been victimized by embezzlers admit they had an inkling that something was wrong, but they didn’t immediately spot the problem. This sixth sense for fraud can be as simple as a vague suspicion or wondering why vendors all of a sudden complain about late payments.
Create policies

Execute a written policy that fraud will not be tolerated and that immediate termination and referral to criminal authorities are the consequences. Add the policy statement to the personnel manual and ask all employees to sign an acknowledgement that they were provided this statement.

Protect the practice further by bonding all employees who have access to the business’ funds. Although the medical practice’s compliance officer is primarily dedicated to preventing fraud and abuse against insurance companies and patients, that officer can also play a role in internal financial fraud. The medical practice’s compliance plan should outline where employees can go to report suspected wrongdoing — including fraud — by other employees.

Stop signature stamps

Get rid of all signature stamps and create a process where all checks written on the medical practice’s account are routinely reviewed by a financial officer. Having that stamp creates the opportunity for an unscrupulous employee to mark financial documents for personal gain. Electronic images of signatures — not to be confused with a secure electronic or digital signature — pose the same problems and should be avoided.

Some banking services can help medical practices reduce the opportunities for financial fraud. For example, using a commercial credit card to pay vendors, instead of writing checks, can increase the oversight of those payments. A commercial bank card can allow the medical practice to institute spending controls for each authorized card user. Ask commercial card vendors if they can provide online reviews of card activity and liability insurance for card misuse.

Manage financial records

The potential for financial fraud is heightened when one individual has access to the medical practice’s bank accounts and controls all of the information about that account. Prevent this opportunity for fraud by segregating banking duties. Ask the bank to send account statements directly to the medical practice’s accountant or to an individual not involved in the transactions.

Banks can offer account reconcilement services to help prevent many types of check fraud. For example, a bank’s account reconcilement service can match check serial numbers and amounts and then generate a report that lists paid checks, outstanding checks and checks that were voided or had stop-payment requests.

Using a high quality color laser printer, it’s not difficult for individuals to slip near perfect-looking checks into an organization’s cash system. Many banks offer services that automatically compare the serial numbers of issued checks with the checks presented to the bank. By transmitting that information electronically to the bank, a medical practice can make those comparisons daily. The medical practice can quickly spot non-matching items that might indicate a fraudulent transaction or perhaps an expensive mistake.

True stories of medical practice fraud

- Front desk supervisor routes end-of-day credit card payment processing directly to her bank account.
- Accounts payable clerk processes payments directly to his personal account using a sham vendor name.
- Lead nurse establishes a company to purchase supplies and equipment, which she then purchases for the medical practice at steeply marked-up prices.
- Biller processes refund checks to various family members and friends who are patients of the practice and facilitates discounts for patients with overdue balances if a concealed, direct payment is paid in exchange.
- Practice administrator shifts payroll deductions from physicians to his bimonthly paychecks, thus receiving a large tax rebate from the IRS after filing his taxes.
While taking these steps can help spot suspicious transactions, it is also important to conduct periodic random audits of payments made to vendors, patients and employees. A common scheme for defrauding medical practices involves a dishonest employee and a dishonest vendor or patient. Medical practices have reported employees scamming hundreds of thousands of dollars by operating companies that purchase products or services from legitimate suppliers and mark up those prices. A more common plot is for the dishonest employee to process refund checks from the practice to the sham company, which is actually a front for a conspirator.

Another favorite tactic of embezzlers is to set up a sham company with a name that sounds like a vendor from which the practice would buy services; anything from a temporary staffing agency to a medical supply company. The consistent link is that the company is owned by the embezzler or a conspirator.

In addition to reviewing bank, credit card and other financial account statements, regularly restrict online banking access to the practice’s accounts. Typically, this access is limited to the physician president, a chief financial officer or other trusted financial managers. In all cases, be sure to change passwords frequently and do not make a written record of those passwords.

Control cash

The front desk at a busy medical practice may collect as much as $10,000 each day in time of service payments from patients. This money can come in the form of checks, credit and debit card payments and cash. As the medical practice encourages its staff to collect more cash, it is critical that foolproof cash controls are in place. Make sure to log and total all money collected at the end of every work shift. Maintain locked cabinets (with limited access to the key) and keep minimal cash on site. Require that the medical practice’s petty cash drawer be balanced every day. Never tolerate discrepancies between the log and the cash count.

Receipts help prevent fraud. With cash flowing into the practice from thousands of patients making payments, fraud can occur when an employee destroys the record of the visit and pockets the cash. Instruct staff to issue receipts to every patient, including those who pay with credit cards. Keep copies of receipts and match them by name or some other identifier in the daily patient log. This may help spot any patients who somehow didn’t pay or, perhaps, did pay but were never credited by mistake or on purpose.
Deploy automation

Using a bank’s remote deposit and automated check clearinghouse services are also excellent ways to prevent fraud. For example, checks written by patients can be converted electronically into debits when they are collected, instead of waiting for the paper check to get deposited and handled by the bank. This type of service speeds up the medical practice’s cash flow and reduces another source of potential internal fraud—dishonest employees pocketing patient payments. Additionally, a remote deposit service can save time and money because a staff member no longer has to make bank runs.

A clearinghouse service can allow the medical practice to securely establish debit arrangements for patients’ payment plans. Plus, the same service allows a medical practice to electronically credit employees’ personal bank accounts ensuring payroll runs smoothly.

The bank might also offer a way to block and filter check transactions. This type of service can spot and reject unauthorized credit and debit activity. Many banks establish the service to screen all transactions so only pre-approved vendors are paid or to automatically flag checks for higher-than-usual amounts.

<table>
<thead>
<tr>
<th><strong>DO</strong></th>
<th><strong>DON’T</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign accounts receivable tasks and accounts payable tasks to different employees</td>
<td>Have incoming mail, receipt counting and daily cash deposits handled by the person who also posts receipts against receivables</td>
</tr>
<tr>
<td>Separate patient billing and bank depository responsibilities</td>
<td>Have the person who does accounts payable duties also reconcile bank statements</td>
</tr>
<tr>
<td>Develop policies, procedures and protocols related to all aspects of cash management</td>
<td>Fail to deploy technology to support your efforts to reduce embezzlement (remote deposit, check clearinghouse, lockbox and others offered by your bank)</td>
</tr>
<tr>
<td>Require that all staff associated with handling cash or financial accounts take periodic vacations</td>
<td>Allow physician owners to take a hands-off approach to understanding the business and financial position of the practice</td>
</tr>
<tr>
<td>Occasionally make changes in responsibility with no advance notice (to expose or prevent collusion between dishonest employees)</td>
<td>Establish a bad example by allowing the practice’s owner or partners to borrow money from petty cash or cash receipts</td>
</tr>
<tr>
<td>Have account reconciliation completed by an employee who does not handle cash or maintain accounting records</td>
<td>Hire employees who handle cash or accounting duties without conducting careful background screening</td>
</tr>
<tr>
<td>Bond all staff who handle refund processing or collect cash, checks and/or credit cards</td>
<td>Allow just one employee to handle all of the practice’s financial activities</td>
</tr>
<tr>
<td>Retain professional outside expertise familiar with healthcare financial and operational issues to establish appropriate financial controls, safeguards and separation of duties</td>
<td>Overlook “red flags” of embezzlement (employees with extravagant living standards, who work overtime, never take vacations and take accounting books home)</td>
</tr>
</tbody>
</table>
Establish a lockbox

Lockboxes offer similar value to prevent fraud and save money. A lockbox directs check and credit card payments from patients, insurance companies and other sources to a special post office box that only receives these payments. The bank’s courier service will pick up payments and deposit them daily into the practice’s bank account.

Not only does this help prevent internal fraud but may increase cash flow. The practice’s staff no longer has to take the time to sort these payments from the other mail, then tally and deposit them. In some medical practices, these tasks don’t get completed daily, and banking deposits are made just one or two times a week, greatly slowing down vital cash flow.

Additional features of a bank lockbox account might include scanning the documentation of payments to give the practice quick online access to deposit activity. Posting of these deposits can go even faster when the bank uses an optical character recognition system to read and process these deposits. A bank’s lockbox also can give customers online access to images of any checks submitted for payment or remittance.

A bank that offers expanded data capture service designed especially for the needs of healthcare providers can be a real plus. This service allows insurance companies to send payments and remittances for patient claims directly to a lockbox where they can be more quickly deposited and credited to the medical practice’s account. The bank scans the checks, explanations of benefits and associated details.

Watch account adjustments

Today’s pricing system for healthcare services creates opportunities for fraud in the billing office of medical practices. Contracted price adjustments can make a medical practice especially vulnerable to fraud by an employee who controls the adjustments, as well as other transactions. Here’s how it can happen: an employee might record the correct price for the service and collect that amount but then post a payment lower than what was collected. The transaction can be made to appear “complete” if the employee records an adjustment that was higher than the actual one and pockets the difference.

Another adjustment scheme involves receiving payments on old accounts. Instead of recording that payment, the employee writes off the account as bad debt while pocketing the payment. Either way, the patient — or the medical practice — is none the wiser. The way to prevent this form of fraud is to restrict authorization for making account adjustments and conduct spot checks of all employees who process those adjustments.
Taking these steps into account, many medical practices realize that preventing fraud is quite a task. While adding more controls may seem like just another way to increase administrative overhead, that expense will more than pay for itself by preventing costly fraud. Savvy medical practices also invest in periodic audits of their internal controls. These can be performed by an accountant or an auditor who specializes in detecting business fraud. Because all practices are different, it is important to consult with a financial advisor for specific advice on how to detect and prevent fraud. Even with controls in place, many medical practices that catch employees embezzling do not bother to prosecute. It’s embarrassing to be a victim, but trying to hush it up by firing the embezzler while not pressing charges just sends the problem along to another medical practice.

With so many medical practices that do not have sufficient internal controls over cash, embezzlement in healthcare continues to be a growing problem. The solution is to implement strict internal controls and to call in the authorities whenever an embezzler is detected.