4 steps to prevent embezzlement, fraud

By Donald P. Lewis, DDS, CFE
Consultant, AAOMS Committee on Practice Management and Professional Staff Development

Fraud and embezzlement in healthcare are crimes causing growing concern. As a matter of fact, embezzlement has become one of the nation's favorite financial crimes. The cost of white-collar crime in the United States is staggering and increasing every year.

Recent reports have losses due to embezzlement and fraud as high as $500 billion annually. That is roughly half the projected cost of healthcare reform!

Unfortunately, oral and maxillofacial surgery practices are not immune to this type of crime. Some practices have been financially ruined due to this silent enemy. These perpetrators not only cost jobs but also important healthcare delivery. They are enemies of oral and maxillofacial surgery practices.

Even though newspaper articles chronicle different types of fraud and embezzlement schemes every day, many have not had any experience with an embezzler. But employee theft is rising, and taking precautions can help avoid this crime happening to you.

The true danger of embezzlement is that it is indicative of larger weaknesses in your practice – you are not just losing income that is rightfully yours. With any type of fraud, your patient data integrity, payer information and historical records (if you use an EHR) are all compromised.

There are four critical steps you can take to monitor your business processes and employees more closely.

What is fraud?

Anything from a small amount of cash taken from a deposit to an elaborate scheme of "lapping" accounts to loss of data by computer fraud are considered fraud losses. Of course, strong feelings about your personal/business income are normal and can be very motivating to protect your practice assets.

But a truly secure practice is required by law to protect the assets of its patients as well. You may know some data losses are prosecutable by law, but you need to be aware you can be prosecuted if you are not taking sufficient measures to protect sensitive information.

In practices connected to the internet, all manner of vulnerabilities threaten patient health and payment data when a practice does not properly ensure hardware and network security – and sometimes even when it does. Under HIPAA, you are federally mandated to protect your patient data. This is not so with your personal and business income.

Fortunately, building simple controls into your practice management and accounting systems can help forestall embezzlement and fraud in your office. The proper internal controls may document incriminating evidence, helping estimate your losses for recovery purposes or even prove a crime was actually committed.

Of course, no practitioner wants to run his or her office like a boot camp. But if you have a built-in system of controls, administer it fairly and tightly, and audit it frequently. You may prevent fraudulent activity that can lead to losses.

Before you can protect yourself, you need to become familiar with some common fraud methods. Dishonest employees succeed in theft because they are trusted with sensitive information. In many cases, the embezzler has been given more authority than the position calls for. Their methods of embezzlement are limited only by the imagination.

Methods and symptoms

Fraud – similar to an oral surgery problem – has signs and symptoms. An increase in patient refunds might represent a concealment of accounts receivable payments. Unusual bad-debt write-offs or an unusual amount of accounts turned over to the collection agency also may signal a cover-up. Declines in practice gross income or profits can be legitimate, or they may be a sign that cash is being stolen. Unauthorized data exports may signal an electronic breach. These symptoms are simply red flags that something abnormal is going on. To diagnose the cause, you need to know the possible diseases.

Skimming

In one of the simplest embezzlement schemes, cash received from a patient's payment is simply "skimmed" or removed from the practice and remains in possession of the thief. This is done without making any record of the transaction. A scam of this type is extremely difficult to prevent or detect. No cash is recorded as an entry and therefore is not shown on the accounts receivable records.

continued on next page

To reduce this type of scheme or the temptation to perpetrate this fraud, pre-numbered invoices or cash receipts should be used at all times when receiving cash in your practice. These receipts are used regardless of the amount of cash being paid. Spot checks also can help assure cash received is actually being recorded.

Lapping

In a more elaborate type of embezzlement scheme, the computer can be used as a tool of the crime. A scheme commonly known as "lapping" is instituted. This involves the temporary withholding of receipts, such as payment on accounts receivable. These payments can be in the form of cash, check or credit card. The lapping scheme usually starts with small amounts of missing funds, but as the scheme becomes more complicated, the amounts typically increase until the embezzler is caught.

Lapping requires the employee to have control of many different aspects of your practice. For example, the employee involved in the lapping scheme opens the mail, receives the cash or checks and is responsible for payments on the open accounts. But how does the lapping scheme work? Let's take a simple look at one.

Patient A makes a payment of $100, and this payment is not entered and is stolen by the embezzler. To avoid suspicion, $100 is then taken from a $200 payment of Patient B. Patient A's account is then credited the $100, and the embezzler pockets the extra $100 without entry. Now Patient B's account is off $200, which the embezzler has taken.

The embezzler may look at this newfound income as only borrowing. The intent may or may not be to repay this debt. The embezzler continues to steal increasingly larger amounts of money involving more accounts.

A fraud of this nature can run for years. It will require detailed recordkeeping by the embezzler in order to keep track of the shortage and transfer it from one account to another to avoid suspicion. Any indication an employee is keeping personal records of business transactions outside your regular books of accounts is a red flag and should be looked at. This scheme will continue to increase in amounts taken, culminating with the embezzler either purging accounts in an attempt to remove the trail, or the embezzler finally getting caught in his or her own web.

Usually an embezzler who is carrying on a lapping scheme also will have access to the accounts receivable records and patient statements. He or she may alter the statement sent to your patients. Thus, the fraud can continue for a long period of time until something unusual happens. A patient complaint may bring the scheme to light. Or this crime may surface through a simple audit of the patient's statements compared with the total accounts receivable.

Payroll fraud

Payroll fraud is another source of lost income to your practice. Occasionally, an enterprising embezzler has added the name of a relative or fictitious individual to the office payroll and collected several paychecks instead of one. They may even increase the gross pay and keep the net pay the same, all the while waiting for the income check to arrive to "collect the bonus."

Data loss, exploitation, identity theft

Loosely protected medical data are a prime source of information for identity thieves. Be aware you are liable if your patient data are not protected, and charges can even be brought for negligent business practices. Data hackers and thieves can access your system and export your patient data to discs, unmarked spreadsheets in your own system, online services set up to host data or even just email data exports to themselves.

Once exported data go online, they are virtually impossible to trace or get back – dishonest employees know this. Your practice management system should be able to show you what reports have been run in the past and what data have been exported. Unauthorized data exports may indicate a loss of data integrity. Be aware of what data permissions level each of your employees has, and limit any data export, email and storage permissions to as few employees as possible. You need to understand and monitor frequently any systems that have access to patient data or allow export or external storage.

Additional guidelines are available under HIPAA, and a savvy practice management software will have reports for you to monitor data transfers and integrity.

Red flags

If employees responsible for the payment entry, accounts receivable, billing and collection are the same employees responsible for patient complaints, they will be able to avoid detection for many years. The amount of shortage can reach such levels that the employee will not dare take a vacation for risk of detection. Your practice should have a policy requiring regular vacation to keep some "indispensable employee" from dispensing with your practice assets.

Employees can always figure out ways to defraud an unsuspecting employer. Other fraud methods include accepting "kickbacks" from suppliers by over-ordering supplies and waiting for the refund check to arrive at which point the employee accepts and cashes the check after forging the payee's name. Personal items can be bought and charged to the practice. The employee may undercharge friends and relatives for services performed. False vouchers and bogus receipts can be used to conceal theft from petty cash accounts. Overtime can be falsely recorded.

Moreover, quite substantial amounts of money can be lost from the cumulative effect of such seemingly minor abuses as personal use of office postage, supplies, equipment and magazine subscriptions. More elaborate schemes have seen defrauders set up dummy companies and falsify documentation of fictitious purchase transactions to collect the payment from the office. As previously mentioned, these schemes are only limited by the imagination.

Four steps to better protect assets

So how can you make your office fraud-proof? Four specific steps will help you on the path to full transparent documentation of business practices. When implemented, these steps will help you both prove transparency and sound business practices to authorities and add to the paper trail of fraud if you suspect illegal activity.

- **Set a good example.** It is easy to see that an employer who frequently helps himself or herself to petty cash, is careless with insurance/payment processing or does not restrict access to important records sets an example of loose business behavior and indifference to the well-being of the practice assets. An established policy of enforced accountability will discourage dishonest activity and advise employees they should know their jobs and feel trusted, but they also are accountable for the records and information that pass through their position.

- **Use a complete practice management software system.** In order to enforce the first step, this second step aids accounting capabilities to help document records, evidence and losses. One potential obstacle to filing a fidelity loss claim is proving the amount of funds that were lost or stolen. You must be able to support all loss claims with evidence of the facts and figures from your records. A good practice management system will help with this if it contains or integrates with electronic accounting systems for managing patient payments and insurance claims.

  Even better, your practice management system should require each employee to log on individually when working with records or data. You can set each employee's password level to sensitive practice information, ensuring limits on access and enabling you to easily monitor individual employee activity without requiring exhaustive reporting. Of course, the proper data backup is just common sense.

- **Have your certified accountant set up recordkeeping.** Be sure to test it for reliability and accuracy by regular independent audits. Your accounting system should have certain minimum capabilities. An audit trail that reports all financial transactions transpiring since the last audit trail was printed should be presented to you every day. These audit trails need to be reportable by user and dated and numbered for accuracy.

  Any audit trail that is not numbered is not an accurate representation of the report requested. Any unusual or unexplained variations should be discussed with the employee involved or your accountant. This will alert potentially dishonest employees you are taking a proactive approach to the financial well-being of your office.

  Another crucial element of proper recordkeeping is a strong electronic backup system that must be in place should anything happen to your physical records. In recent years, electronic recordkeeping has become standard business practice, not only for ease of use and space saving, but because electronic systems can be backed up with remotely hosted services should disaster strike your physical practice. Your primary practice management system should feature – or at least integrate with – this tool as a minimum requirement. Additional precautions should be taken to ensure any records not controlled by your practice management system also are protected electronically.

continued on next page

■ **Separate the duties of all employees.** In particular, separate the duties of those employees who prepare the daily cash deposits and those who receive the cash and checks. Basically, no individual employee in your practice should handle any transaction from the beginning to the end. For example, the employee who receives payments from patients (either in person or through the mail) should not be the same employee who is responsible for making the bank deposits. This includes accounts receivable and accounts payable transactions. Be sure you get a duplicate bank deposit slip from the bank, and do not be afraid to make the bank deposits yourself on a routine basis.

A few other common-sense business practices will strengthen your systems and enable you to monitor processes further:

- Check the background of prospective employees whether or not they are going to be involved in the handling of the financial portion of your office.
- Be aware of any changes in financial or personal problems with your employees. Employees living beyond their means are all too common in embezzlement cases. Also, employees with personal or financial problems may take advantage of loose business practices to help their own situations.
- Be sure no one is placed on the payroll without prior written authorization from you.
- Arrange for all bank statements to be sent to you directly and unopened. If there is concern in these regard, they can be sent to your home or a Post Office Box.
- Personally examine all canceled checks and endorsements to see if there is anything unusual. Make sure the bank returns your canceled checks and not just the statements.
- Spot-check your patient records and their corresponding financial accounts. This will let your staff know you are interested in the financial well-being of your practice.
- You should have direct responsibility for any bad debt or uncollectable write-offs.
- Do not delegate the signing of checks and approval of cash disbursements, and never approve any payment of an invoice without proper, accurate and original documentation of the transaction.

Steps help to minimize risks

These four principal steps will help you minimize the possibility of your practice falling victim to this white-collar crime. Each step is critical, each is dependent on the other to be effective and each could alert you sooner to the possible perpetration of fraud.

If you are troubled by the red flags you are seeing, do not jump to any hasty conclusions. What at first may appear to be a clear-cut case of fraud or embezzlement may be nothing more than weak internal controls with a perfectly valid explanation. Institute controls immediately for optimum visibility into potential weaknesses.

If it becomes apparent you have good reason to suspect a crime, contact your attorney immediately for guidance through the proper steps to proceed. In our technology-dependent healthcare environment, data fraud or theft is just as serious as financial embezzlement, and immediate involvement with the local law enforcement authorities is of utmost importance. Prosecution is paramount and not prosecuting could constitute charges against you, and even leave you vulnerable to further attack.

In summary, no legitimate "busyness" claim will compensate if you are eventually victimized by this silent crime. Time, diligence and processes must be applied to ensure you and your practice assets are as safe as possible. Not one control will guarantee your safety against a determined perpetrator, but the proper system of controls will protect your employees, your practice and, ultimately, your career and family. ■

This is number 164 in a series of articles on practice management and marketing for oral and maxillofacial surgeons developed under the auspices of the Committee on Practice Management and Professional Staff Development and AAOMS staff. Practice Management Notes from 2002 to present are available online at AAOMS.org.