PRACTICE MANAGEMENT
NOTES
A Supplement to the AAOMS Today Newsletter September/October 2009

Four easy steps to prevent embezzlement, fraud and data compromise

By Donald P. Lewis, Jr., DDS, CFE

Introduction

Fraud and embezzlement in health care are crimes of growing concern. 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 each and every year. Recent reports estimate losses due to embezzlement and fraud as high as $500 billion annually. That's roughly half the projected cost of national health care 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 Perpetrators cost not only jobs but also important health care 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 OMSs have not had any experience with an embezzler. Employee theft is rising, and the reason why is still being debated by security experts. They are split over whether the economic downturn is making the problem worse by raising the tension between employers and employees. The true danger of embezzlement is that it is indicative of larger weaknesses in your practice. You're 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. Here, fraud and its methods and symptoms are discussed, as 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" (defined later) accounts, to loss of data by computer fraud, is considered a fraud loss. 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 that some data losses are prosecutable by law, but you need to be aware that you, too, 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 doesn't properly ensure hardware and network security—and sometimes, even when it does. Under HIPAA, you are federally mandated to protect your patient data. Not so with your personal and business income.

Fortunately, building simple controls into your practice management and accounting system can help to forestall embezzlement and fraud in your office. The proper internal controls may document incriminating evidence, which will help estimate your losses for recovery purposes, or even prove that a crime was actually committed. Of course, no practitioner wants to run their 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 we can protect ourselves, we 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 their position calls for. Their methods of embezzlement are limited only by their imagination.

Methods and Symptoms

Fraud, like an oral surgery problem, has signs and symptoms. An increase in patient refunds might represent a concealment of accounts receivable payment. Unusual bad-debt write-offs, or an unusual amount of accounts turned-over to the collection agency, may also signal a cover-up. Declines in practice gross income or profits can be legitimate, or 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 that is 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. To reduce this type of scheme or the temptation to perpetrate this fraud, prenumbered 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 can also help assure you that 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 and continues, 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 a lapping scheme work? Let's take a look at one.

Patient A makes a payment of $100 and this payment is not entered into the practice records 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 with $100 and the extra $100 is pocketed 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. Their intent may or may not be to repay this debt. They continue to steal increasingly larger amounts of money involving more and more accounts. A fraud of this nature can run for years. It will require detailed record keeping by the embezzler in order to keep track of the shortage and transfer it from one account to another to avoid suspicion. Any indication that an employee is keeping personal records of business transactions outside your regular books of accounts is a red flag and should be investigated. This scheme will continue to increase in amounts taken, culminating with the embezzler either purging accounts in an attempt to remove the trail, or finally getting caught in his or her own web.

Usually an embezzler who is carrying on a lapping scheme will also have access to the accounts receivable records and patient statements. They 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 the crime may surface through a simple audit of the patient's statements compared with the total accounts receivable.

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

DATA LOSS, EXPLOITATION AND IDENTITY THEFT. Loosely protected medical data is a prime source of information for identity thieves. Be aware that you are liable if your patient data is 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 e-mail data exports to themselves.

Once exported data makes it online, it's 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 has 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, e-mail 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.

Under the Red Flag Rule, physicians who offer or maintain covered accounts are considered creditors, and are required to develop, implement and main-tain a written identity theft prevention program designed to detect, prevent and mitigate identity theft. Savvy practice management software will also include reports for you to monitor data transfers and integrity. Please note that there are additional requirements to protect patients' information and identities that fall under the scope of HIPAA and the impending Red Flag Rule. You and your mana-gerial staff should review both on a regular basis.

SIGNS OF POTENTIAL FRAUD IN YOUR PRACTICE. If the employee responsible for the payment entry, accounts receivable, and billing and collection is the same employee responsible for patient complaints, then he or she 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.

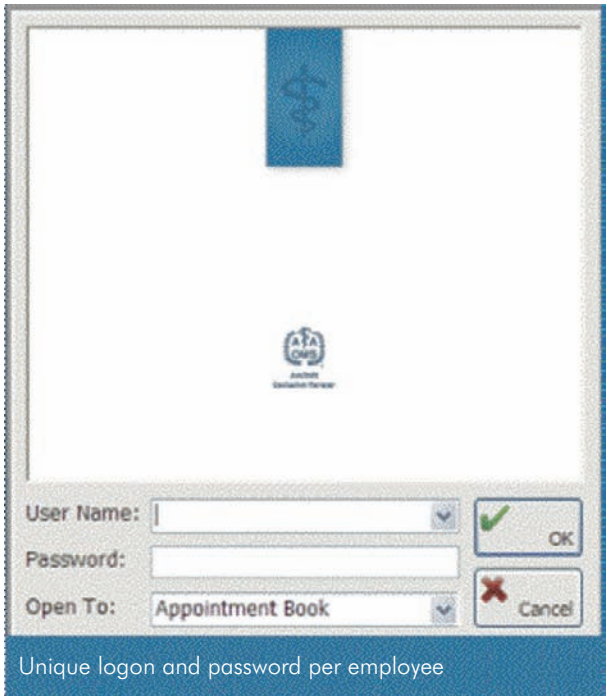
Employees can always figure out ways to defraud an unsuspecting employer. Other fraud methods include accepting "kickbacks" from suppliers by over-ordering supplies and waiting for the refund check to arrive, at which point the employee accepts and cashes the check after forging the payee's name. Personal 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, 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, as well as charging personal long-distance phone calls from the office. 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 limited only by the imagination.

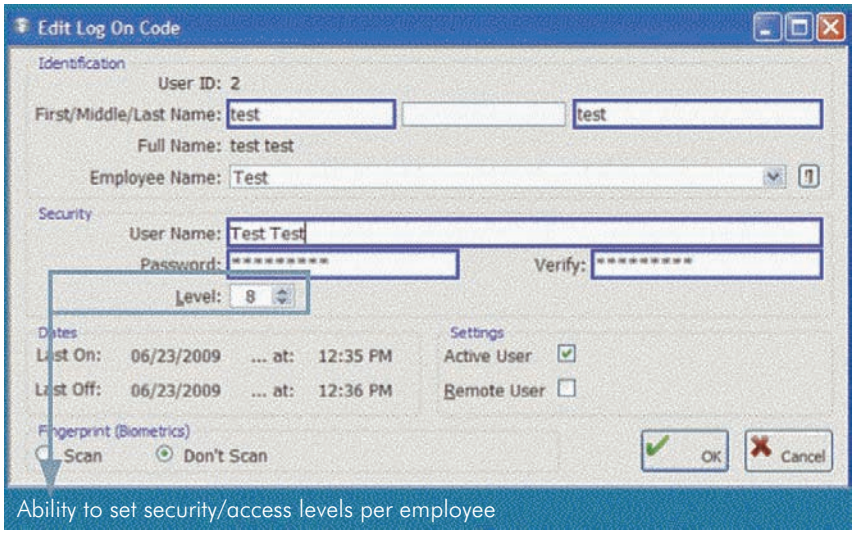
Only You Can Prevent Office Fraud: 4 Steps to Better Asset Protection

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.

First and foremost, you as the practitioner/employer should set a good example. It's easy to see that an employer who frequently helps him/herself to petty cash, is careless with insurance/payment processing, or who doesn't 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 that, while they should know their jobs and feel trusted, they are also accountable for the records and information that pass through their position.

Second, in order to enforce the first step, use a complete practice management software system with 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.



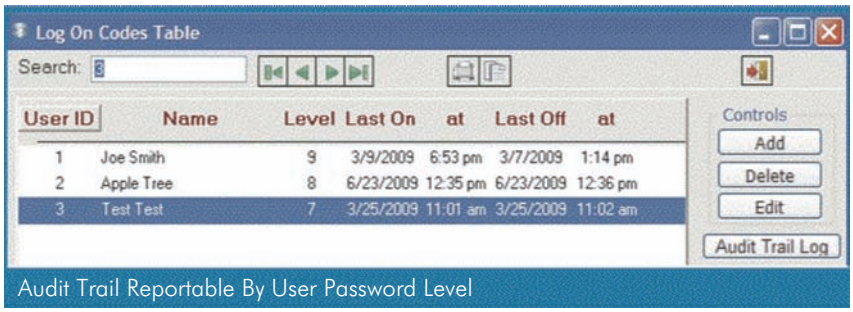


Ability to set security/access levels per employee

Your primary practice management system should feature or at least integrate with this tool as a minimum requirement, and additional precautions should be taken to ensure that any records not controlled by your practice management system are also protected electronically.

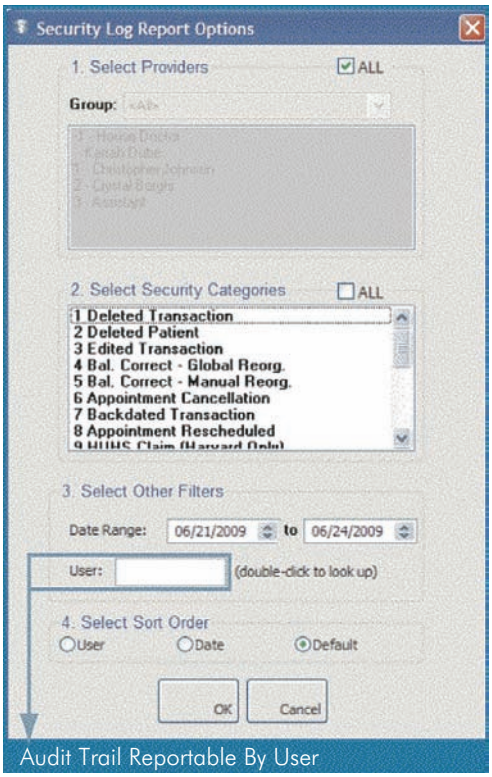
Fourth, separate the duties of all employees, in particular, those employees that prepare the daily cash deposits and those that receive the cash and checks. Basically, no one individual employee in your practice should handle any transaction from the beginning to the end. For example, the employee who 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. Make sure that you get a duplicate bank deposit slip from the bank and don't be afraid to make the bank deposits yourself on a routine basis.

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



Audit Trail Reportable By User Password Level

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 that you are taking a proactive approach to the financial well-being of your office.



Audit Trail Reportable By User

Another crucial element of proper record-keeping: strong electronic backup systems must be in place should anything happen to your physical records. In recent years, electronic record keeping has become standard business practice, not only for ease of use and space saving, but also because electronic systems can be backed up with remotely hosted services, which could prove invaluable should disaster strike your physical practice.

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

- Check the background of any prospective employee, whether he or she is going to be involved in the handling of the financial portion of your office in accordance with your state laws.
- Be aware of any changes in financial status or of personal problems of your employees. Employees living beyond their means are all too common in embezzlement cases.
- Make sure that 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 this regard, they can be sent to your home or to a Post Office Box.
- Personally examine all canceled checks and endorsements to see if there is anything unusual. Make sure that the bank returns your canceled checks along with the statements.
- Spot-check your patient records and their corresponding financial accounts. This will let your staff know that 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, ever approve payment of any invoice without proper, accurate and original documentation of the transaction.

Summary

The four principal steps discussed here 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 the warning signs you're seeing trouble you, don't 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 transparency of potential weaknesses.

If it becomes apparent that you have good reason to suspect a crime, contact your attorney immediately for guidance through the proper steps to proceed. In our technology-dependent health care 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 failure to prosecute could result in charges against you, and 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 that you and your practice assets are as safe as possible. No 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.

Dr. Donald P. Lewis Jr. is the chairman of the AAOMS Committee for Software Development and Computer Technology and is a Certified Fraud Examiner.

CALL FOR AUTHORS:

Interested in submitting articles for consideration for the *Practice Management Notes* series? If so, please contact Ms. Beth Hayson at bhayson@aaoms.org. Possible topics include, but are not limited to: financial management, legal, marketing and practice building, office and personnel administration, practice organization, regulatory requirements and retirement/estate planning.

This is number 112 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 Allied Staff and AAOMS staff. *Practice Management Notes,* from 2002 to present, are available online at *aaoms.org.*

Whatever your practice needs, AAOMS has a product that can help. And, during the month of September, you can obtain these premier practice management resources at a 25% discount!

Billing and Reimbursement Manual
~~$40.00~~ **$30.00**

Maximize your reimbursement levels and minimize claim-filing hassles! This manual shows you how it's done.

Insurance Manual: A Guide to Understanding, Filing, and Appealing Claims
~~$195.00~~ **$146.25**

A perfect complement to the Billing Manual, this resource includes procedure-specific flow charts of the appeals process, as well as sample form letters.

Office Design and Construction Manual
~~$165.00~~ **$123.75**

Whether you're redesigning space or building from the ground up, this manual contains the information you need to assure everything is up to code and primed for operating efficiency.

Practice Management Manual
~~$165.00~~ **$123.75**

Every practice day brings innumerable management decisions. Whether it's establishing office procedures, overseeing staff or marketing your services, let this manual help you enhance your management skills.

Don't miss this chance to improve your practice management — and, take it easy on your bottom line!

Order online at aaomsstore.com

American Association of Oral and Maxillofacial Surgeons
saving faces | changing lives®