FACTS ABOUT FRAUD

Fraud, Theft, & Embezzlement: Recognizing & preventing fraud in your practice Part 2

March 2019

The statistics are scary! As we wrote in our February 2019 newsletter, fraud, theft, and embezzlement can happen to anyone at any time. A 2014 AAHA study reported that 86% of practices that responded had identified employee theft in their hospitals. Some might say the other 14% just hadn't discovered the theft – yet.

Warning signs

One common warning sign of embezzlement is when a practice is profitable but has unexplained low cash flow. Like in the example in our February newsletter, the practice is growing more every year, but always seems to have trouble paying bills. It turned out the office manager was embezzling from that practice.

Mounting credit card bills can also be a warning sign. In that same example above, the office manager charged many of her personal expenses on the company credit card. She recorded each charge in QuickBooks, but the vendor name was different from what was on the credit card statement.

Unusually high payroll runs also warrant review. Verify that hours worked and rates of pay are correct and compare them to the previous payroll cycle. Where are the differences and do they make sense? Verify that employees receive the correct amount of vacation and haven't increased hours without your consent.

Inventory is another area highly susceptible to theft and fraud. If you are constantly off when you reconcile inventory, have a lot of discrepancies or can't seem to account for missing items, you may have an employee with "sticky fingers." Employees aren't the only people who may steal from you. The culprit could be a client, a vendor or even the pizza delivery person. Inventory reports should match the quantities in stock. If they don't, it isn't the fault of the practice management software; it's almost always the result of human errors. These errors usually aren't intentional, but if there are no consequences for being "off", the problem will not only persist but will multiply.

If reconciliations of day sheets, bank accounts, inventory or petty cash are routinely off, or rarely happen, take the time to understand why. Banks do make mistakes, but not consistently and rarely for large amounts.

How to prevent fraud

The easiest way to prevent fraud is to separate duties and establish checks and balances. "Internal controls" are the protocols and systems in place to protect your assets, ensure accurate financial reporting and promote efficient and effective operations. Here are some examples of internal control procedures you should have in place.

- Reconcile the daily reports from the practice management software to the cash, checks and credit card slips each day. The employee doing this reconciliation should sign off on the daily report to confirm who did the work. Locate and correct discrepancies before the bank deposit is made, and have a different person take the deposit to the bank.
- Limit check signing duties to only the practice owners. If you need an alternate signer, have the owner's spouse be a signer. Never sign blank checks.
- The person placing inventory orders should be different from the person receiving and verifying the orders. A front desk person could verify the order in a small practice.
- If payroll is prepared in-house, the practice owner or CPA should review payroll before it is submitted. If that is not possible, review and corrections should occur immediately after.
- Divide the check writing, check recording, and bank reconciliation duties between two or more employees. That helps ensure that it will take collusion between them to write fraudulent checks. Be sure that each employee understands he or she will be held accountable for the procedures each is assigned, and each has an obligation to ask questions about items that seem unusual in any way.
- Reconcile bank and credit card statements within a week of receipt. Thefts have sometimes been disguised because no one reconciled the statements in a timely manner. Once a practice gets behind on these reconciliations, it's easy to stay behind and keep fraudulent transactions hidden.
- Limit access and issuance of company credit cards and strictly enforce company credit card policies. Take advantage of business credit card programs that work with only certain vendors or categories, and would "decline" purchases at places that are not typically for business use, such as liquor stores or The Sunglass Hut.
- Within your practice management and accounting software, utilize and assign appropriate security roles and rights, and frequently review and update them. Make sure that no one has the ability to delete anything. If a mistake needs to be corrected, implement an approval process that requires at least two people, including a manager or owner, to execute the correction. In one case, an employee had the ability to delete invoices, so he was pocketing the payment he collected from the client and then deleted the invoice in the software.
- Review manual adjustments to your clients' accounts receivable in your practice management software. If a client makes a cash payment on an outstanding receivable, an employee pocketing that cash must adjust the client's outstanding balance or run the risk that the client will complain.
- Incorporate careful hiring practices and run background checks on potential employees. A veterinary hospital in the Midwest hired an employee who began stealing from the practice after just 6 months on the job. They later discovered that the employee had a long history of theft. Had the hospital run an inexpensive background check before hiring, they could have prevented a lot of heartaches and saved a lot of money, too. Closer to home, Summit contacted a candidate's former employer for a reference. The candidate indicated that the owner had retired and closed his business. In fact, the business was going strong and there was an arrest warrant out on the candidate for embezzling funds.

In no way is this list complete. Even the best systems aren't foolproof. There will always be a few people looking for new ways to beat the system. Something that can appeal to the consciences of that 80% of people who may or may not steal from you, is simply to be involved. Walk around your practice, be seen in the pharmacy, sit with the bookkeeper and review the numbers. Even if you don't fully understand it all, make an effort to ask questions and learn. Your simple attention to finances could deter an employee who is considering stealing. In staff meetings, talk about integrity and honestly and clearly communicate that there is ZERO tolerance for anything less! Set a good example with your own behavior.

If you suspect fraud

Conduct a ***discreet*** investigation and gather as much evidence as possible. If you need help, involve only those that are in a very small circle of trust. For example, a practice owner expressed his suspicions and concern about his office manager to an associate veterinarian, who told his technician, who told the receptionist, who then told the office manager. The owner's suspicions were accurate, but because word got back around to the office manager, she had time to destroy evidence before she could be caught.

Once you have hard proof, consult an employment attorney or the police. They will advise you regarding the best way to approach the employee, and what options you have for resolving the problem. Immediately start the legal process of prosecution, repayment plan, or whatever you decide is best for you and your practice. Regardless of how you decide to address the issue, immediately remove the employee from your practice and do not allow them to return. Get their keys and any other company property they have, and change passwords the same day.

We often hear practice owners say "not on my watch", "it can't happen here" or "we are all like family." Unfortunately, many of those same owners saw red flags or warning signs and ignored them because of those misconceptions. No matter the size of your practice, there are internal controls, processes, and systems you can implement in order to protect you, your employees and your practice.