www.hcplive.com/physicians-money-digest/practice-management/Sound-Internal-Controls-are-Vital-to-Your-Practices-Health

# Sound Internal Controls are Vital to Your Practiceâ€™s Health

Author: Stephen A. Pedneault

There is a shockingly high probability that your medical practice will become the victim of a theft by one of its own employees. In fact, studies show that this is true for an estimated 40% of medical practices. Although it's surprising, it doesn't mean it's inevitable. Practices that review their financial policies, implement preventive measures and put in detection procedures are far less likely to become victims of a disturbing and growing trend.

Just as the medical community recommends regular physicals for individuals to ensure a healthy lifestyle and detect potential issues early on, every practice should be evaluating their checks and balances, internal controls and segregation of duties to ensure a healthy financial lifestyle, as well as to detect potential issues.

**Why should I act now?**

Given the economy and unemployment, more individuals are under financial stress today than I have ever experienced in my 23 years as a certified public accountant. Combined with the increases experienced in gambling, spending (and spending on credit), individuals living beyond their means and personal addictions, the risk of an employee stealing or embezzling from you is significant. So what can you do to prevent it?

**Mind those collections**

In my 20-plus years experience, the most common and significant embezzlements have been perpetrated against medical practices through their collection processes. I expect these kinds of thefts to become even more prevalent in the future. The reason is that banking is becoming more automated. Today, an increasing number of deposits can be made remotely via images versus physical checks. That makes fraud schemes involving the diversion of payments much easier to accomplish.

The typical medical practice receives payments in a variety of ways. Keeping track of them is becoming increasingly more complicated. Is your practice part of a group with multiple locations? If so, depending on the financial tasks performed at each remote location, you can expect the risks of employee theft to escalate. Does it have a number of ancillary revenue streams, such as non-covered elective self-pay procedures or products it offers for sale? This means the number of potential risk areas grows again.

Payments may be received directly at the practice or processed contractually via a bank lockbox arrangement. Sometimes patients pay on the spot for services in full or they may be paying their balances and co-pays during office visits. Collections may be completed in-house or contractually by an outside agency. It all gets tougher and tougher to keep track of the payment streams.

What all this means is that you've got to have controls in place that ensure that the practice appropriately receives all the funds due and that all the funds are properly deposited and credited to the practice.

**It starts with scheduling**

When I evaluate a medical practice's collection processes, I start with a good hard look at their scheduling. Simply put, the collection process starts with scheduling and ends when you've seen the patient, entered and processed the charge, and received, posted and deposited the corresponding payment into the practice's bank account. Sound simple? In reality medical billing and collection is very complex, and there are both internal and external factors that will cause havoc on the process.

Sound internal controls start by ensuring that you identify and enter the charges for services into the billing system on the day the patient receives treatment. Period. You must reconcile each provider's schedule with the appropriate charges, taking into account walk-ins, no-shows and other scheduling issues.

A common scheme for diverting funds has to do with these issues. Here's how it could work: a patient comes in to see the doctor and pays his or her portion of the bill after the visit. But the payment never reaches the doctor's bank account because the perpetrator diverts the patient's payment and marks the patient's appointment as a "no show."

As you evaluate your processes, you have to ask yourselves out loud about these and similar atypical issues that take place every day. How should they be accounted for? How would your practice know if someone exploited one of these issues to conceal their theft?

Secondly, make it a policy to give every patient a written receipt for any payments collected. No exceptions. Use a three-part pre-numbered receipt book at every point of collection. The white copy goes to the patient, the yellow goes in a drawer with their payment to be reconciled for the day's receipts and the pink remains in the book. Regardless of how the patient pays (cash, check, credit card…), he or she gets a receipt from the book. To back this up, post a sign at each collection point that reads, "Expect a receipt for any payment you make today." This puts your patients on notice that they should receive a receipt. The sign along with the receipt book adds a great deterrent to the payment process.

**Payment processing**

Now, let's talk about how you process payments. Whether payments are mailed to the practice or to a post office box, they must be managed by the practice to ensure they are all properly deposited into the practice's bank account. Sounds pretty basic — but this is where most of the theft issues start.

A standard practice found years ago was to prepare a list or tape of the payments received upon opening the mail each day. While this might seem low-tech today, it's really still a good way to handle payments that come through the mail. What makes it an effective way to head off employee theft is that the individual initially processing the payments should have no posting access. This segregation of duties is very valuable.

Here's how it works: once the payments are totaled, they are copied and prepared for deposit. At the same time, the total is sent to the practice manager or an owner. The check copies are then posted, and a payment posting report is generated. The deposit is taken to the bank or completed via remote depositing, and a deposit receipt is returned to the practice. Then, and only then, is the deposit considered complete. The last measure is for the office manager or an owner to compare the posting report with the initial list and the deposit receipt.

For some reason, many practices have moved away from this process, creating opportunities for employees to divert payments and conceal their thefts by posting adjustments to the diverted patient's accounts. This removes the outstanding balance and no follow up will be performed as the patient's account balance will be gone.

In many of the cases I investigate, I've found that dishonest employees can be very creative in finding ways to process payments (checks) payable to the practice to their own personal bank account. It shouldn't happen, but it does. And I expect it to become more commonplace as banking moves towards processing pictures of checks via smart phones and other cellular devices.

**Other ways diverted payments can be concealed**

Like it or not, there are still other ways that those under financial pressure could steal from your practice. Even if payments are reconciled, and all the charges are entered into the billing system for every patient seen, there are still two basic risks that involve adjusting or writing off balances.

Let's talk about adjustments and write offs first. The ability of employees to adjust or write-off patients' balance should be limited to the smallest number of employees possible. Having said that, anyone responsible for posting payments and collection efforts will need this access, as posting adjustments (contractuals) is required of posting virtually every Explanation of Benefit (EOB) received.

The best way to minimize this risk is to have extensive detection measures in place. Make sure your billing system has a very detailed list of adjustment codes (or "reasons" for the adjustments). A report that includes "adjustments by reasons" section should be part of the standard monthly reporting package owners review monthly. The report should identify all the codes, along with the totals posted by code for the month.

Further, I encourage our clients to generate a simple spreadsheet, with each code listed down the left side. On the top of each column is the month. At the end of each month, the amounts by code are entered in that month's column. This makes it easier to do a month-to-month comparison over time. It will also help reveal that someone is inappropriately posting unauthorized adjustments to patient accounts to conceal unauthorized activity, including theft.

**Collections**

Once you have entered the charges and they are transmitted for payment, the patient's unpaid balance remains on the accounts receivable agings until paid, adjusted or written off. Other than what's been discussed here, there are other ways for dishonest employees to divert patient funds. These include leaving unpaid balances of diverted patient accounts open on the practice's accounts receivable aging report, causing the practice's balances to grow both older and larger.

While little can be done to prevent this, much can be done to detect it. Those aging reports can help. The aging should be generated and reviewed each and every month, and you'll need to track the totals for each category (current, 30 days, 60 days, 90 days, over 90 days and total) monthly as well. The month-to-month comparison and trending will help identify a potential issue within your practice's collection process. The underlying cause could be an employee theft, or an employee not performing their collection and posting responsibilities. Each of these can have an extremely harmful impact to a practice's cash flows.

**In summary**

This article is only a start. It hasn't covered all the risks and areas of opportunities within a medical practice regarding collections and cash receipts, where a rogue employee could steal payments. Unfortunately there are many more ways and schemes. However, the areas covered in this article are common, basic and applicable to virtually every medical practice.

What else can you do? Start by asking yourself these questions as a way to identify potential opportunities and minimize risk:

- How do we know we have captured all the charges, sales, and encounters that occurred (for a given provider, on a given day)?
- How do we know that we billed for all the procedures we performed (again, for each provider, for each day)?
- Can there be any exceptions within the process and, if so, what are they and how do they create an opportunity?
- If someone was going to exploit this particular process, what are all the ways they could do it?
- If it were to be exploited, where and how would their exploitation show up?
- For things that cannot be prevented (e.g. not practical to segregate duties due to limited number of employees), focus on detection means. Ask yourself how would inappropriate or unauthorized activity be concealed within each and every area of your practice?
- When establishing measures to review for completeness as well as potentially exploited areas, ensure someone independent of the targeted process conducts that review.

Provider schedules are getting busier, patients' ability to pay is diminishing and reimbursement rates are declining. These and other trends will likely have a significant impact on your practice's cash flows, if it hasn't already. In today's economic climate, it is more important than ever to ensure your billing process is tight, and you collect everything due your practice. The last risk that should be in your equation is whether an employee is stealing valuable and much needed funds from your practice.

*Stephen A. Pedneault is the principal and founder of Forensic Accounting Services, LLC, a public accounting firm specializing in fraud investigations, forensic accounting, employee embezzlement, fraud prevention, litigation support services, internal control evaluations, due diligence analysis, and various other special projects.*