www.hcplive.com/physicians-money-digest/practice-management/Are-Your-Employees-Stealing-From-Your-Practice

Are Your Employees Stealing From Your Practice?

Author: Stephen Pedneault, CPA/CFF, CFE

This is the second of four articles by Stephen A. Pedneault on employee embezzlement.

In my last article, I discussed the staggering rate at which medical practices fall victim to theft and embezzlement, and the critical financial controls needed to combat the risk of an employee crossing the line from working for you … to working for him or herself, at the expense of *your* practice.

I am optimistic that the practice owners who read my first article returned to their practices, spoke with their employees responsible for billing and finances, and evaluated the financial controls in place. If they found those controls deficient, it is my sincere hope the practice owners implemented my recommendations.

But it doesn't end there. Most people believe that if they cover the billing cycle from scheduling through collections, nothing further could happen within the practice's billing cycle. They couldn't be further from reality. Individuals under significant personal pressure to "permit" themselves to steal from their employer will often find other ways to divert funds, conceal their thefts from detection, and rationalize their actions.

What other vulnerabilities exist within billing?
Every practice must deal with patient overpayments, whether created by a third-party payer or by a self-pay double payment. The credit balances reside on the accounts receivable aging report, and, left unattended, over time they can grow into a sizable amount.

Many practices employ procedures to regularly process credit balance refunds, while other practices, particularly those smaller and with fewer resources, allow the credit balances to drop down the list of processing priorities.

Blended with uncollected patient balances, such credit balances can frequently distort the practice's true total outstanding "collectible" balance, and can thus mask another potential issue within ineffective follow-up efforts.

Every practice should regularly monitor and report the accounts with credit balances to ensure timely processing of refunds and to keep the accounts receivable aging as true to the collectible amount as possible. This requires two key controls.

First, supporting documentation should accompany every refund request, just as any other type of disbursement request commonly paid through accounts payable, legitimizing the need to process a payment back to a patient or payer. The check-signer should review each check against the supporting documentation provided, and the practice should retain and maintain the support similar to paid invoices.

Second, refund payments should be processed (i.e. paid) from an account separate from the practice's main operating account. Due to the high volume of payments and the low level of scrutiny over each payee, the chances of a check being processed, diverted, altered and stolen is higher than with regular vendor payments. If paid from a separate designated refund account funded by the operating account, the account could be easily closed should a payment be compromised, and a new refund account established.

The main activity of your practice's operating account (direct deposits, electronic remittances, checks, payroll, EFTs, ACHs and auto debits) will remain unaffected. Conversely, if the practice continues to pay refunds from its primary operating

account, every transaction tied to that primary account would require redirection to a newly established account — creating an administrative nightmare.

Who follows up on the uncollected balance?
The efforts of most practices focus on billing for procedures performed and payment posting (along with adjustments and denials). Frequently, properly billed charges remain unpaid by third-party payers and individuals alike, requiring some follow-up to track down payments on these accounts. In-house collection procedures often include sending out statements, making collection calls and utilizing collection letters soliciting the payment.

Unfortunately, individuals with collection responsibilities have used their positions to divert much-needed funds away from the practice, sometimes simply by changing the remittance address included on statements, collection letters and return envelopes to the employee's post office box. The dishonest employee can adjust the patient's balances off the billing system, thus eliminating any potential future follow-up on those balances.

One collections manager diverted more than $200,000 over two years by simply having return envelopes printed with an address she controlled. She deposited some payments into her personal bank account, while bringing others to the practice for deposit, demonstrating that her collection efforts yielded results … *just not to the full extent of her efforts*.

Do outside collections require controls, too?
Practices also send uncollected balances to outside collection agencies when in-house efforts prove unsuccessful, with the hope that more aggressive collection techniques will yield payments. The balances sent out for collection may remain on accounts receivable, may be re-characterized and segregated from the regular uncollected balances, or may be written completely off the accounts receivable aging.

Performing due diligence over the collection agencies you utilize provides a good starting point. How well do you know them? Who are the owners? What other practices utilize their services? What do those practices have to say about them? How much do they charge? What is their collection reputation?

Your practice needs a procedure to identify and approve all accounts ultimately forwarded to the collection agency. Create a report identifying each individual account, and review, approve and retain it. This critical procedure will monitor the efforts of the collection agency to ensure they work your accounts and remit payment to you.

Here, too, employees have demonstrated impressive creativity in their means to divert funds. A practice manager living beyond her means simply established her own outside collection agency, and, using her position of access and authority, forwarded uncollected accounts prematurely to her own agency. Her collection efforts, typically conducted from home after regular work hours, provided easy money from recently billed accounts, and she only turned up her nose at the oldest and most uncollectible balances on the practice's system — leaving them for the in-house collection effort's pursuit.

Enough about billing — disbursements can also prove lucrative
Every practice makes purchases, approves invoices and processes payments to vendors for goods and services. The two largest areas outside of payroll and benefits (discussed later), both in transactions volume and cost, comprise medical and office supplies.

Critical controls should ensure that every payment relates to an approved expense of the practice. It starts with controls over adding new payees and changing vendor information (the "remit address") in your accounting system. A rogue employee could simply generate a check payable to a legitimate vendor and change the vendor's address to one the employee controls.

While more and more vendor payments occur electronically, whether by EFT, ACH, or simply through on-line bill payments, time-tested controls over physical checks *must* remain in place, regardless of your payment methodology.

First, every check must carry the support of an original vendor invoice or check request form (when there is no invoice). Supporting documents must accompany checks ready for signature by the primary signer, to allow for a review at check-signing time. A great control? Have the check signer add his or her initials to the supporting invoices, thus providing evidence of their review.

Second, the practice should strongly consider implementing check-signing thresholds and requirements. Checks with amounts below the threshold would require only one original signature, but checks for more than the set amount would require two signatures. No signature stamps — ever! Period. These stamps lead to a certain path of problems.

Third, provide vendor payments "mail-ready" to the check signer, so that the signed checks go directly into the envelopes … and off to the vendors. Return the supporting invoices only to the check preparer for filing. Anything less and the risk exists for alteration or diversion of a check *after* approval and signature.

Last, but certainly not least, all of the same control recommendations apply if the practice processes payments electronically, rather than by check. Only authorized signers should possess the ability to disburse funds electronically. Other individuals can have "read-only" access to bank accounts if needed, but they must not have the ability to release funds by *any* means. And, of course, do not share user IDs and passwords. Require separate user IDs for each individual.

Credit cards — what's in *their* wallets?

Far too many practices fall victim to credit-card abuse or embezzlement through the unauthorized or inappropriate use of an employer-issued credit card. This is one area where controls can detect a problem easily and early on, limiting the potential for loss.

First, limit the issuance of practice credit cards to authorized individuals, with as few as possible available. If practical, limit cards to the owners; but remember, your practice could indeed have a problem within that group as well...

Second, policies should require support of any credit card use, i.e., any charge, with an original store receipt. Recurrent missing receipts or no receipts provided? Revoke their card.

Employees with access to cards should have a timely review their statement, attach their receipts and return it for payment processing. Critical accounting capacity should not require chasing down receipts and statements.

Last, the check signer should review the statement with supporting receipts as part of signing checks. This provides a third review of the credit card activity, and initialing the statements validates this review.

Employee reimbursements and petty cash… areas for concern

Properly designed and implemented procedures in both areas can limit potential abuse and embezzlement. Require completion and signature on a form, supported with original receipts, for any requests for funds.

Review the receipts provided. Are they originals or photocopies? Did the employee travel on the dates identified? Did the employee even work on the date he or she reported the mileage incurred? Schemes involving airline tickets and car rental receipts are commonplace. Multiple submissions of the same receipt on different days can occur. One practice manager used receipts previously submitted by her employees, submitting them as her own to support reimbursement checks she paid herself.

Aren't we safe using an outside payroll service?

Recent embezzlements I investigated involved individuals responsible for processing payroll (both internally and through third-party vendors) by diverting funds through schemes within the practice's payroll. Ghost (non-existent) employees, terminated employees paid beyond termination and unauthorized increases and/or bonuses paid to the person who actually processes payroll are all common techniques.

However, payroll fraud creativity apparently knows no boundaries. In one case, the payroll clerk ingeniously manipulated the withholding fields of her payroll. Rather than entering positive numbers, which in turn deducted amounts from her gross pay, she entered negative amounts into the fields, adding unauthorized funds to her "net" pay. Consequently, each pay period, her net pay was double her gross, and, after only four years, she managed to embezzle and conceal nearly $429,000.

Know your employees. Review in detail the payroll registers and reports, looking for anything unusual. Do this each and every pay cycle, just as in times past. Pay particular attention to the payroll details of those employees who have access and opportunity to process payroll. Monitor any changes made to the payroll system, such as new, changed or terminated employees. If possible, export a list of the names and addresses of all your employees and sort the list in Excel to see if any employees have the same address or if key field information goes missing, such as a Social Security number.

If your practice processes payroll in-house, print the payroll registers and reports each pay period, and have someone independent review them in detail. If your practice uses an outside vendor, do the same with their reports. If you can only obtain their reports electronically, print, review and save them, as if you physically received them.

One victim's story

Donald Elton, MD, a victim of employee embezzlement, practices in Columbia, S.C. Elton's experiences as a victim of his employees' behavior inspired him to write the book *How To Steal From A Medical Practice*, as well as sponsor a website focused solely on issues pertaining to preventing or detecting employee theft and embezzlement within a medical practice. Take it from those who know — a book written by a physician practice owner, *directed* to physician practice owners. Good medicine… Physician, Heal Thyself, Indeed!

In summary…

This article completes my identification of many areas commonly exploited by employees within medical practices. Unfortunately, this doesn't cover all identification and discussion of the myriad exposed and vulnerable areas. Wherever your practice receives funds, the potential exists for diversion of those funds … and financial risk to your practice.

What can you do, given the many areas of opportunity? Total security won't arrive overnight. Start by reviewing the major areas discussed and ensure adequate design and implementation of controls, with regular, systematic follow-up to prevent or detect unauthorized activity in each area.

Next, over time, identify and evaluate every financial area of your practice, focusing on one area at a time. The three questions you should ask yourself as part of your assessment of EACH area include...

1. What vulnerabilities exist within this particular area that would allow someone with access and opportunity to steal, embezzle and/or divert funds from the practice?
2. If someone *did* exploit a vulnerability within this particular area, how would they conceal their activity?
3. How could we detect their unauthorized (fraudulent) activity?

Due to the frequency of employee embezzlement, I limited this discussion to identifying key areas and schemes, and implementation of controls and procedures to minimize the related risks.

Prevention and detection both constitute great measures, but one additional measure — the "missing link" — will likely provide any practice the best chances of recovery … but only if implemented.

My next article will focus on providing this "missing link," completing the discussion preventative measures. Then we will proceed into how practice owners should react when they first identify potential signs or symptoms of theft or embezzlement.

What should you do when you think you've discovered employee theft, and, more importantly, what should you NOT do? Your action (or inaction) may create more risk to your practice than the actual theft itself…

Much as the patient who receives a potentially serious diagnosis, the best advice remains to proceed with prudence but also with caution, and obtain the timely advice of professionals and possibly specialists who can direct you in your action … and perhaps inaction.

Part One

More reading:

Sound Internal Controls are Vital to Your Practice's Health

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. A forensic accountant, Steve is also certified fraud examiner, certified in financial forensics and a forensic certified accountant. He is an author and frequent public speaker on issues related to fraud. He has authored or co-authored three books on the subject and is currently working on a fourth. For more information, see: www.forensicaccountingservices.com.