SPRING 2012/Vol.19/No.1

WWW.PHYSICIANSMONEYDIGEST.COM

Physician's MONEY DIGEST®

Putting Finance Into Practice for Physicians

PLUS

FINANCE

CHOOSING THE RIGHT FINANCIAL ADVISOR

PRACTICE MANAGEMENT

SUSPECTED EMBEZZLEMENT? WHERE DO YOU START?

TRAVEL/LEISURE

NEW YORK AUTO SHOW

PRESIDENT NICOLAE CEAUSESCU'S PALACE

European Must-Sees

History at your feet

We think an employee is stealing from our practice. *Where do we start?*

By Stephen A. Pedneault, CPA, CFE

Prevention and detection measures are critical to combating employee embezzlement, but to truly fight the risk of fraud the practice must effect a third element: insuring against a potential loss due to employee theft. Maintaining adequate "employee dishonesty coverage" could likely serve as your only means for recovering diverted funds when prevention and detection measures fail.

Where to Start? Educate Your Employees

In so many cases of employee theft and embezzlement at least one other employee or co-worker knew of wrongdoing. Those types of details often surface when interviewing all the employees as part of an investigation. Had the employee acted on his or her knowledge or suspicions, the practice would have suffered a contained loss.

The problem in these instances is there are no policies, procedures or means for employees to communicate their information to someone in a position to do something about it without jeopardizing their own employment. Worse, the practice never communicated to employees their obligation to report any information related to any potential wrongdoing to allow the owners and/or management to investigate the issue.

Merely telling employees they have a duty to forward indications of potential theft or wrongdoing will not suffice. The practice must provide specific channels for employees to communicate the information, and the employee handbook or personnel manual must include a description of these channels and how to use them. These documents must confirm the assurance of an employee's anonymity. For example, many employers use an independently monitored 1-800 "fraud hotline."

Using a bona fide independently monitored hotline ensures zero risk to the employee of caller ID, as the person monitoring received calls has no relationship to the practice. Further, while the service gathers, transcribes and communicates the information to the practice's owners or management, it does not provide or retain the actual call.

*This is part of a series of articles by **Stephen A. Pedneault, CPA, CFE**, on discovering and preventing employee embezzlement. The previous installments can be found on PMD's website.*

Potential Fraud Rears Its Ugly Head

Take this example. While conducting routine follow-up procedures on outstanding balances within accounts receivable on your billing system, the representative from the carrier identifies that the patient balance in question (unpaid on your system) was previously paid to the group several months ago.

Was the payment received? Did the check get lost in the mail? Or, perhaps, did payment get applied to the wrong patient balance? These are all common possibilities in this scenario. The representative provides the payment date, and the billing system cannot locate any payments for that carrier around that date. Your collections person expands the inquiry to other outstanding patient balances with that carrier and provides them to the representative. Unfortunately, each one shows up as previously paid and no longer outstanding (uncollected) on your system.

Unaware of why the practice's system does not reflect the carrier's payment, the collections person requests a copy of the carrier's payment, front and back. Simultaneously, the collections person informs the practice manager (or a physician owner, if no manager) of the discrepancy.

Speculating on what could have happened can prove problematic, so the practice should keep the issue quiet until it receives the check image. If a diversion scheme exists, identifying the perpetrator could prove difficult if not impossible with such limited information.

Conducting detailed inquiries and interviews with the staff involved with billing and collections could tip off a fraudster to their scheme's discovery, causing him or her to delete and destroy any trails, along with supporting evidence he or she retained of the crime.

Or it could reveal a legitimate and credible explanation, such as the inadvertent sending of a carrier's payment check to the wrong medical practice, something the other practice's controls should have detected and prevented, but did not. Under that scenario, the employees would never know of the issue, thus avoiding any unnecessary negative impact on employee morale.

While the potential for diversion may exist, many other explanations common to medical billing could prove the case. The carrier may reveal the check existed, but never cleared their bank. The check could therefore have disappeared in the mail or within the practice's processes. Either way, the practice could request a replacement payment of the carrier.

While waiting for the payment images to arrive from the carrier, someone could discreetly look into any other patterns of unpaid balances with other carriers.

Are there any trends? Are unexplained unpaid balances found across all carriers, or restricted to certain carriers? Often practices have several large payers, such as Medicare, Medicaid, Blue Cross and Aetna, who account for the majority of revenue, as well as many smaller payers.

Thefts from the larger carriers may prove difficult for employees due to the sheer size of the payments and because many remit their payments electronically, eliminating the opportunity to steal their payments.

Most small practices continue to receive checks from many smaller payers. Concealing the diversion of a $50,000 payment from Medicare,

accompanied by a 10-page Explanation of Benefits (EOB), would prove far more difficult than skimming several smaller checks, each less than $2,000 from other payers with less volume, whose EOBs may only include a few patient accounts.

Patience and Persistent Will Prevail

After hounding the carrier's representative to follow up with their research department to get you the image needed of their payment, you finally receive it. The check, payable to the practice, has cleared the carrier's bank.

Unfortunately, when you flip the check over, in place of the presence of the practice's endorsement stamp, the check contains no endorsement ("Endorsement Absent Deposit Guaranteed"). The check encodings identify the banks as First Atlantic Bank and Pioneer Bank (both fictitious for this article). The check is drawn from a Pioneer account, explaining that encoding, but the practice does not have any known bank accounts at First Atlantic Bank. Who received and processed the check paid to the practice, and where did the funds go?

Do you now have evidence that an employee has perpetrated fraud against the practice? It's very much a possibility, but not the *only* possibility, and so uncertainty remains.

What *do* you know? That the carrier's check cleared a bank not used by the practice. A request of First Atlantic Bank may provide you the answer you seek ("Whose account did the check clear?"), but likely not. If the bank account in question belongs to anyone other than the practice, then the bank cannot identify the name or nature of the account.

One solution? Contact the carrier to alert them of their check's diversion and request the issuance of a replacement check. The problem will then shift to their fraud department, and the practice will obtain its funds. However, if a theft issue resides within the practice, the remedy for the replacement check will not provide any further information supporting or refuting that potential.

A little discreet due diligence can also help determine if a fraud problem exists.

Start by identifying all the employees with potential access to the payment. Then, with human resources, review those employees paid via direct deposit to see if any of the employees have their paychecks deposited to an account at First Atlantic Bank. If so, certainly you should further investigate those employees. If no direct deposits exist, consider reviewing any past reimbursement checks issued to employees, and if you can obtain images, see if any of the checks cleared First Atlantic Bank. Ultimately you may need to engage counsel to get you the information needed of First Atlantic Bank.

Simultaneous to all these efforts, you should review all the unpaid accounts to identify other balances for confirmation with other payers or carriers. Follow-up procedures, including calling the carriers on those accounts, could identify other instances where your practice sent a payment not received or recorded on the practice's system. If you identify one or more checks as not received, you likely have an internal problem.

Evidence of Potential Fraud Confirmed. So Now What?

Once you find the potential for fraud, theft or embezzlement, the first thing every medical practice must do is contact counsel. Prudent, independent and objective legal direction and advice will pay dividends and minimize additional risks and exposure.

Frequently, other "ancillary" issues could prove a greater risk to the practice than the theft itself. Most importantly, engaging counsel to direct and oversee all investigative activity will provide a layer of confidentiality by ensuring attorney-client privilege over all work performed. Suffice to say, you need to contain the information known among the fewest people possible.

Schedule an initial meeting as soon as possible with counsel, outside the practice if possible, so as to not alert employees potentially involved. During that meeting, the practice and counsel must work together to identify a strategy on how to move forward, confirming or refuting the potential fraud, as well as determining "who," "what schemes," "how," "how much" and "how long" of the fraudulent activity. Much of this may prove indeterminable at the initial meeting, so avoid speculating beyond the known facts and information. A major discussion point should detail how the practice will preserve key information and evidence to minimize the risk of loss through destruction or diversion.

Concurrently, the practice should locate and review insurance policies, identifying any possible coverage in place. Commercial packages often include employee theft and embezzlement (commonly called "employee crime").

One of the most important areas of the policy comprises the section entitled "Your duties in the event of a loss." Typically small in size, this section identifies the four to five steps the insured (the practice) must take to preserve, file and collect on a claim against the policy coverage.

The first step almost always requires the insured to notify the insurance carrier in a timely fashion of the "potential" for a claim. Many refer to this as "putting the carrier on notice." A claim may ultimately not be filed, but in order to preserve the option to file a claim, the practice must provide timely notice.

So what do you tell the carrier? My advice: Little to nothing, because you probably don't know much more at that point. Anything further exists as mere speculation. The policy requires notice, so provide nothing more.

Also insist that the carrier mail you a written acknowledgement that you provided timely notice and start a potential insurance claim file. If sent via email, print and preserve their emailed acknowledgement. I am a big proponent of counsel dealing directly with the insurance carriers on behalf of the practice.

With counsel on board, evidence preserved and the insurance carriers put on notice, you now have time to execute your strategy and planned procedures.

You may need other professionals to aid in the investigation and preparation of the resulting insurance claim (if warranted), such as fraud examiners, forensic CPAs, medical billing experts and forensic computer specialists. The practice's counsel overseeing the matter should directly engage every outside professional brought onto the investigative team to ensure the attorney-client privilege governs their work.

Risks and Exposure: What NOT to Do

Reacting without thinking and planning can often prove costly. Many precedents and much litigation exist to support this. Performing procedures without possessing proper qualifications and prior experience can have a negative impact on the practice.

Shows like *CSI* and *Law & Order* have unexpectedly created a sense of empowerment known as the "CSI Effect."

One practice manager, so "empowered" by television, yet unprepared for the meeting by not having completed any investigative measures to define the extent of the potential problem, attempted to solicit a confession from a staff member. The unsuspecting staffer admitted to an amount specified by the manager (an amount much smaller than subsequently proven stolen).

Unlike many cases where that critical interview constitutes a one-time opportunity, the manager subsequently found more evidential transactions, confronted the individual for a second time, and he admitted to the higher amount. The practice manager discovered still more, leading to a third and fourth admittance.

Finally, my firm became involved, and put a stop to the ad-hoc interrogations. Each successive meeting with the suspect created added risks to the practice. The practice should have placed the staffer on administrative leave, preserving the one-time opportunity for a confession once the team quantified the extent of the scheme.

Keep the "circle of trust" small. Hold all information and conversations in confidence. Don't speculate. Remind those in the know of their duty to keep things quiet, private and confidential.

"Too Many Cooks..."

Another risk occurs when too many individuals gain knowledge of the potential fraud and investigation.

Rumors start. Misinformation spreads like wildfire, often finding its way back to the targeted individual, exposing the practice to the potential of a slander or libel lawsuit if the investigation ultimately clears the individual of any wrongdoing.

Commonly, some employees often have relationships among themselves unknown to the other employees within the practice. Someone placed on paid or unpaid leave during an ongoing investigation may receive information through their internal sources. A tactic of planting disinformation to exploit this connection could prove useful as part of the practice's strategy, but only after careful consideration with counsel.

In one case, our investigative team wanted the individual on leave to learn of the discovery of their scheme and supporting evidence. Selected employees, made aware of a "mole," frequently discussed planted "details" of the investigation within his earshot, which likely led to the information making its way to the suspected employee. Psychology plays into financial investigations much more so than most would know.

Keep the "circle of trust" small. Hold all information and conversations in confidence. Don't speculate. Remind those in the know of their duty to keep things quiet, private and confidential.

Prepare a script of what you will tell others within the practice regarding the proceedings. Counsel should have a big role in preparing your script. Have another script for what you will tell patients, vendors and others if they ask, especially if the targeted individual holds a highly visible position within the practice and is placed on leave.

Plan for the Unexpected ... *and* the Expected

The advice of counsel will once again prove invaluable when other issues crop up after your investigation reveals an employee diverted funds from your practice, especially should the amount prove significant.

You must conclude the responsible individual's employment, either through voluntary resignation or through involuntary termination. An employee who decides to resign creates the least risk to the practice, especially if the resignation includes releases and "hold harmless" provisions. Present the employee with that option, as some actually choose to resign. For all others, you must terminate their employment. I highly recommend a detailed letter drafted by counsel articulating the termination, and it should include a demand for the immediate return of any and all property of the practice.

On the day you conclude the individual's employment, expect that former employee (and thief) to file for unemployment benefits. Identify a plan of response with counsel, and prepare to prevent further financial impairment by allowing the individual to collect benefits — on your dime.

That said, I caution you not to use the unemployment hearing or process to try your case of theft against the individual. The former employee will crave information, as will his or her attorney, and you should endeavor to give them little to nothing, given your likely ongoing investigation.

Next will come the time to fund the practice's retirement plans, and decide whether the employee who stole funds qualified as an eligible participant at the end of the most recent plan year. You will need to discuss funding the employee's contribution, but, in the end, the risk of blowing up the practice's retirement plans will outweigh the cost of funding the individual's account.

Something to consider if talks have started with counsel representing the former employee: have the individual's retirement accounts voluntarily frozen and made available down the road as a means toward restitution. You generally cannot seize retirement assets, but the individual can voluntarily sign them over.

A sharp defense attorney (or experienced fraudster) may try to get you to negotiate a resolution, offering to begin repayments toward the diverted balance. If a victimized practice accepts any type of repayment or deal, it will likely remove the option of criminal proceedings as law enforcement and prosecutors interpret this as reaching a civil agreement (many criminal justice agencies will seek out any reason to avoid taking the case).

A better plan would see counsel accepting into client funds any money the suspect is willing to start accumulating toward restitution. This way the practice makes no agreement or settlement, and it doesn't accept any funds. Rather, funds are simply being accumulated within an attorney's client funds account, money that may (or may not) be accepted toward some resolution down the road.

What Else Can You Expect?

Individuals accused of fraud often bring complaints or suits against the victim employer. In some instances, the issues raised may carry credibility, albeit separate from their acts of theft, but in most cases, the allegations constitute a mere distraction to divert attention away from the thievery.

One physician group determined one of their providers diverted funds by altering billing records and changing the provider codes for posted procedures. Shortly after discovery, investigation and substantiation, the group terminated the physician.

As discussions began on what to do with the investigation results, the practice was served with notice of a lawsuit. The former provider claimed the practice's general partner sexually harassed her and created a hostile workplace environment. Although no evidence could be found substantiating the claims, the practice incurred significant fees to defend the claim.

My experience substantiates that most fraud suspects file unsubstantiated claims, mainly to distract from their acts of theft.

Working with Law Enforcement

Here's my opinion: We should arrest and prosecute anyone who steals. Get it on their record and get it in the media, so the next employer will know. *Caveat Emptor* — let the buyer (potential subsequent employer) beware.

However, each crime proves unique. As part of the strategy discussion with counsel, the practice owners need to weigh the risks and benefits of criminal pursuit. Additionally, realize that your insurance policy may require the involvement of law enforcement.

Keep in mind that law enforcement's primary goal consists of making an arrest and successfully prosecuting a crime. While you can request restitution, it is uncertain, and in some jurisdictions no enforceability provisions exist within the criminal system to enforce the restitution order.

Other Critical Considerations

In many cases, the fraud or embezzlement committed within a medical billing environment is not limited to the practice's funds. Many villains create billing schemes to divert fraudulent proceeds or to conceal diverted funds, creating massive exposure.

Compliance with Medicare, Medicaid and all the other payers' contractual requirements could all constitute risk exposure, leading to the potential to return funds fraudulently received by the practice (and worse, unbeknownst to the physician owners). Not only will the practice lose the diverted funds, it may have to repay any payments it was not entitled to receive. This could define the end of the practice and expose all the physicians to federal and state investigations, as well as compliance audits from every participating payer.

The importance of contacting counsel as soon as the practice detects the first sign of a potential problem and ensuring counsel oversees the entire investigation cannot be overstated. The practice must protect these discoveries under the attorney-client privilege, to further discuss how best to report and resolve each issue.

In Summary...

For every case of a practice falling victim to employee fraud or embezzlement that becomes public, eight more exist that do not, mainly due to the risks and issues to the practice discussed in this article.

Recently, I learned that an embezzler whom I investigated and successfully had arrested last year had gained employment at a well-known, high-profile institution. So here's my question: If this individual's previous employer terminated her, criminally charged her and her status of pending adjudication in that arrest stood as public record while she applied for the new position, *how* on earth did she get that new job?

Accordingly, my final article in this series (available online in August 2012) will discuss practical measures and procedures every employer should implement and follow in screening applicants for hiring.

In my experience, the recidivism rate for financial crimes runs high, and individuals with past experience *will* apply for job openings within your practice. Do NOT let them in.

Until then ... remain vigilant.

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 a 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. For more information, see: www.forensicaccountingservices.com.*