PHYSICIAN STRATEGY GROUP

SERVING THE USPI PHYSICIAN NETWORK

Let's make a plan to thrive.

Fraud Within Healthcare

Fraud - A Global Problem

According to the Association of Certified Fraud Examiners' 2010 Fraud Study, organizations lose ~ 5% of their annual revenues each year to fraud. That equates to a potential world-wide loss of $2.9 Trillion.

- Asset misappropriation (i.e., theft) accounts for 90% of fraud cases, with a median loss of $135K
- Small organizations are more vulnerable to fraud
- More than 85% of fraudsters had never been previously charged or convicted for a fraud-related offense
- Fraudsters frequently display warning signs of their illicit behavior such as living beyond their means & experiencing financial difficulties
- Frauds are more likely to be detected by tip than by any other means

Embezzlement – A Physician Practice Problem

According to a survey of the Medical Group Management Assoc, almost 83% of physician practices have been victims of employee theft/embezzlement. One fourth of those surveyed reported $50K or more was stolen. But these fraudsters' activities can also cause compliance problems

- Incorrect/false claims
- Privacy violations
- Identity theft of patients or physicians
- Inaccurate/incomplete medical records

Examples of Fraud

The following frauds have occurred over the past several years.

Sharing these lessons learned is a powerful way we can help prevent such frauds from happening again.

Accounts Payable Embezzlement – $490k

After the business office manager at a small ASC was terminated for unrelated reasons, management discovered that she had been writing manual checks to fraudulent vendors and had been manipulating payee information on checks printed from the AP System. This fraud precipitated the removal of check stock and the mandate for all AP checks to be printed from an off-site location.

Controls that failed:

Bank reconciliations – Accountant was trying to work with BOM to address all the paid-no-issues but did not escalate the problem to management. As a result of this fraud, a bank reconciliation escalation process was implemented

Positive pay – this bank account feature was not activated on the bank accounts at the time, which would have prevented the cashing of any checks that had not been recorded in the AP system and transmitted to the bank

Check signing authority – the BOM initially had check signing authority, but after basic segregation of duties were put in place and she was removed, she asked the clinical director to sign blank checks prior to printing them "since she was so busy"

Vendor statement reviews – BOM was receiving all vendor statements and vendor complaints for non-payment so no one else in management could see the growing outstanding vendor balances

Payment Posting and Suspense Account Fraud

The BOM at a large facility directed the payment poster to post future receipts in the current month prior to month-end close in order to meet cash collection goals because she had an incentive bonus based on meeting monthly cash collection goals. The poster was posting anticipated payments based on phone calls to the No EOB suspense account.

Controls that failed:

Bank reconciliations – Accountant was trying to work with BOM to address all the deposits-in-transit but did not escalate problem to operations management.

Daily balancing of deposits to patient accounting system payment batches

Periodic review of the No EOB/suspense account

Collector Cash Theft - $270k

Without management's knowledge, a long-time collector was negotiating balance settlements with patients if they paid in cash. Although she was not authorized to accept patient monies at all, this collector was counseling patients in her private office and maintaining her own cash receipt book. While she was out on vacation, a patient who had received a statement complained that he had already paid $300, and the separate cash receipt book was discovered in her desk.

Control that failed:

Adjustment approval – collector was obtaining supervisory approval of adjustments for reasons such as bankruptcy or hardship without the necessary supporting back-up

Access restrictions – collector had full system access to post adjustments without any approvals or oversight

Payroll Embezzlement - $37k

The payroll processor at a large facility was embezzling via payroll using a variety of methods: (1) changing PRN employees' direct deposit accounts to her own bank account and adding time in the payroll system for pay periods not worked, (2) giving herself unauthorized pay increases, and (3) adjusting PTO balances and failing to process PTO hours for personal vacation time taken.

Controls that failed:

Supervisory time approval – supervisors were not signing off in payroll system for hours worked by their staff, and especially not for the payroll processor's time.

Review of personnel change report – review of this report would have identified activity such as payrate changes for the payroll processor, deletion of health insurance deductions, and an unusual volume of bank account direct deposit changes

Review of payroll register – review of this report would have identified pay for PRN employees who had not worked in that pay period and fraudulent pay for the payroll processor. Reviewers are also instructed to specifically review and sign off on the payroll processor's pay per the payroll register for reasonableness of hours, payrate and deductions

Expense Report Embezzlement - $40k

The payables processor entered unapproved and unsubstantiated expense reports for him/ herself into the AP system for payment. This fraud precipitated a modification to list additional payee details, including address information.

Controls that failed:

AP system invoice entry – payables processors are trained to never enter unapproved invoices into Oracle for payment although there is no system control to prevent them from doing so

Preliminary payment register review – a thorough review of the proposed check run prior to authorizing the checks to be printed should have uncovered expense reports on the list that the admin had not reviewed & approved

Expense report approval – the admin approved some of the payables processor's expense reports without sufficient review because these reports were later found to include overstated mileage and unsupported or non-business expenses

Cash Theft - $5k

Business office staff were collecting up-front cash from patients then pocketing it. In some cases, they also wrote off the patient's balance in an attempt to hide their theft.

Controls that failed:

Physical cash controls – cash box was unlocked during the day and located in an unsecured drawer where most employees had access

Cash segregation of duties – the individual collecting patient monies also prepared the deposit slip, and in some cases also posted the payments in patient accounting system and reconciled the cash receipt book

Daily cash balancing – reconciliation of daily deposit log to deposit slip and cash receipt book would have promptly identified the missing funds, except in the case where segregation of duties was inadequate

Online Banking Embezzlement - $105k

The BOM had on-line access to a separate bank account for the facility's billing company that was not managed and accounted for by USPI. She used this access to pay personal credit cards and other bills over the course of almost two years. In addition, she and the materials manager opened a Sam's Club account in the facility's name but used the card only for their own personal purchases.

Controls that failed:

Bank account on-line access – the BOM and payables processor should never have more than read-only access to any cash disbursement accounts for the facility

Bank reconciliation – no one other than the BOM reviewed the monthly bank statements and no one independent was reconciling the bank statement to the accounting books (i.e. Oracle & AdvantX)

Preliminary payment register review – a thorough review of the proposed check run prior to authorizing it should have identified Sam's Club purchases on the list that were not made for facility business purposes

Fraud Red Flags

- Are there any employees who haven't taken vacation in a long time? If so, they may feel the need to work continuously to keep covering their tracks.
- Does anyone employed by the practice maintain unusual working hours? The employee in one of the scenarios above was coming in after hours and working late when all other employees were gone
- Does any employee have a non-standard incentive bonus based on specific financial results that could be easily manipulated or misstated?
- Does anyone employed by the company maintain an extravagant lifestyle compared to his/her salary and financial means? The employee in one of the scenarios above was a single mother making $40k a year in a depressed area of the country but driving a Hummer and leasing an expensive house

Fraud Red Flags (continued)

- Is anyone employed by the company exhibiting signs of an addiction (drug, alcohol, gambling, etc.)? The employee in one of the scenarios above had a gambling addiction and had wracked up some significant debts

- Do credit checks for potential hires or promotions to management reflect any concerning issues such as substantial debt or collection activity? One of the employees in a scenario above had gambling problems and a high debt to income ratio per his credit check. As a result of this fraud, Recruitment developed a new background and credit check matrix that sets thresholds for certain credit report activity

- Does any employee have a private office and work frequently with the door closed? This might be an indication that he or she is doing something inappropriate and trying to hide it

Controls to Combat Fraud

Some controls help to prevent fraud from happening. These are examples of Preventive Controls:

- *Background checks & drug screens for potential hires*
- *Tone at the top of honesty & integrity*
- *Zero tolerance policy communicated to staff*
- *Perception of strong management oversight and controls*
- *Physical safeguards over cash and other physical assets*
- *Segregation of duties*
- *Restricted access*
- *Mandatory vacations*
- *Authorization levels*

Controls to Combat Fraud

While other controls help find fraud quickly. Here are some examples of Detective Controls

- *Daily balancing*
- *Account reconciliations*
- *Whistleblower hotline*
- *Periodic physical inventory counts*
- *Financial statement reviews*
- *Supervisory review of payroll, AP, account adjustments, etc.*
- *An alert & fraud-trained staff*

Physician Strategy Group

follow up questions or comments:

Phone: 855-207-5230
Email: info@upsi-psg.com

www.physicianstrategygroup.com