

Preventing employee theft, embezzlement

October 28, 2015

By [Lisette Hilton](#)

There are many ways in which employees and even fellow physicians can steal and embezzle from an medical practice, according to Jay A. Shorr, BA, founder and managing partner, The Best Medical Business Solutions, Fort Lauderdale and Orlando, Fla.

“I do forensic accounting, and if I go into a practice, and there is a thief... I’ll find them,” Shorr says.

Cosmetic dermatologists and others whose practices perform a lot of fee-for-service procedures are particularly vulnerable, according to Shorr, who presented “Banishing Employee Theft and Embezzlement in Your Office,” yesterday at the Global Aesthetics Conference, in Miami Beach, Fla.

Among the big areas of employee theft: time, supplies and cash. Some employees, including aestheticians and midlevel practitioners, will charge for procedures inside exam rooms and collect for those separately.

“When insurance pays revenue, it goes through the third-party portal or a clearinghouse, and then the insurance companies pay money directly into the banking account of the medical practice. However, when you’re a fee-for-service practice, you can either steal product (skin care products and supplies), or you can steal money,” said Shorr, who is certified as a medical business manager and aesthetic consultant.

It’s usually not the big-ticket items, such as surgeries, because the higher fees for those procedures are easy to spot as missing. Rather, employees will often steal revenues from small, non-invasive procedures or services, he says.

In one typical scenario, a patient will have Botox. The employee will post the transaction and the patient will get a receipt for payment. The employee will then go in and delete the transaction and pocket the cash.

“The daily report at the end of the day comprising of cash, checks, and-or credit cards will match because when you’ve deleted the transaction, it deletes the amount of money that should go into the bank,” Shorr says.

In some cases, employees will take loans from the practice. How? A patient pays cash and the employee takes the cash and charges the same amount on his or her personal credit card. The practice cash and credit card report amounts match at the end of the day and the employee walks out with a free loan, gets the credit card points, while the practice has to pay the merchant fee to the credit card company.

NEXT: [Tips for Preventing Theft](#)

Tips for Preventing Theft

Theft and embezzlement prevention lie in vigilance, according to Shorr who says that physicians should audit their transactions. If there are an inordinate number of credit card transactions, do some digging and check the merchant copies of the receipts.

“If you have the same truncated numbers for the credit card number (last four numbers of the credit card) on multiple receipts, or a rather large credit card purchase that does not match any individual transaction, that’s a red flag,” Shorr says.

To check for and detect deleted transactions, make it a point to know which patients were seen that day. Go into the patient record of your practice management system and make sure they're all documented.

Here's a creative tactic: Someone affiliated with the practice opens a bank account with a similar name, of the practice and is the only authorized signer. When checks come in, some go to the legitimate account, while others go to the sham account. Sometimes, the thief will create dummy invoices for office supplies and have the practice pay the amount into his or her account. The best way to prevent this from happening is to know your vendors and audit your invoices to make sure all transactions are going through the right account and to the real vendors.

A final thought: "Don't always rely on the same person to do the checking. Check the checker, in case the checker [is] the thief," says Shorr.