Et tu, Brute?

JOHN SHUFELDT, MD, JD, MBA, FACEP

In the past, when I have broached the topic of employee theft with urgent care owners, their typical, somewhat indignant, response is, "My employees would never do that!" I really like this answer because I really value loyalty – more than anything. In the film *Ides of March*, campaign manager Paul Zara (Philip Seymour Hoffman) proclaims: "I value loyalty over everything." Of course, he completely gets screwed (by his former employee) at the end of the movie but at least he can look himself in the mirror every morning — so he has that going for him, which is nice!

Here's the rub. If no employees would ever do this why is one out of three business failures in the United States the direct result of employee theft?[1] Truth be told, this has happened to me – twice. Both times the perpetrators were discovered and ultimately fired. The first time we recovered the money ($70,000); the second time was a much smaller amount and we did not recover the money. Both of the employees went to work for competitors—and the second one sued us.

One trait common to medical providers is that we think people are honest and will generally do the right thing and, that no one (particularly a trusted member of the team) would knowingly steal or be disloyal to us. Yet it happens all the time.

Here are some steps that will help you prevent employee theft:

Make the Right Hire

Check references. "Had I known" should not be coming out of your mouth when you find out that your employee has been dishonest. Ask around about a prospective employee–and not just the people someone has listed as references. Urgent care medicine is a small community and chances are, someone you know will know the prospective employee and give you a straight answer. In addition, if the job requires handling money, get the potential employee's permission in writing to check his/her credit report.[2] I am not sure you can draw any linear conclusions but desperate times sometimes lead to desperate measures. In the same vein, doing a criminal background check and verifying employment history is absolutely integral.

One rule of thumb is to separate cash collection functions from payment and deposit functions.

Trust your gut. Applicants who "trash talk" a previous boss, leave with little or no notice or state that previous co-workers did not like them because of _____(fill in the blank) should be a red flag. One caution: If an applicant discloses some personal information to you about a potential disability, marital status, pregnancy, religion, etc. you cannot refuse to hire him/her for that reason. Be careful. I know of situations in which prospective employees have related something on purpose just so that if they weren't hired they could claim it was due to the issue they disclosed.

Keep notes during the hiring process. This way, if it goes "south" you will have something to fall back on to stimulate your memory. Occasionally, applicants will pad their resume or make grandiose statements about their past. (I recently had an applicant tell me she had a ride in an F-35, which I found interesting since a two seat F-35 has never been made. Wait, could she have meant an F-350 Ford? I better check my notes! Whew, she said "fly."). Needless to say, she was not hired.

Institute a probationary period. A 90-day probationary period is always a good way to "test drive" an employee for a period of time and it allows the employee to "test drive" you and the company. Another option is to make the initial hire as a consultant with payment as a 1099 independent contractor. If no red flags appear, the consultant can be hired as a full-time employee.

An Ounce of Prevention

There are a number of procedures and internal controls you can institute to make it more difficult for an employee to steal or

John Shufeldt is principal of Shufeldt Consulting and sits on the Editorial Board of *JUCM*. He may be contacted at *Jshufeldt@Shufeldtconsulting.com*.

embezzle from the practice. One rule of thumb is to separate cash collection functions from payment and deposit functions. (This is what caught me in the first episode). In addition, have the bank statements mailed directly to you at a different address. If something does not seem correct, start researching it. Here are some additional internal control procedures:

Check bank statements. As discussed above, check them yourself and see where the funds are going. Look for odd patterns, vendors who don't seem to have a role in health care, and unexplained fluctuations in deposits.

Monitor work hours and vacation time. One pattern I have witnessed is staying late, coming in on weekends, and irregular work hours to help hide embezzlement. If you see someone "working hard" you are less likely to suspect him/her. However, this is typically when the embezzlement is taking place. In addition, require employees to use their vacation days. That gives you some time to check their work. Rotating roles occasionally is a great way for employees to learn other aspects of the business. It keeps them on their toes and gives them perspective on the entire organization. It also allows others to review their counterpart's work. If an employee is reluctant to have others review his/her work, that's a red flag.

Discuss insurance that covers employee theft and embezzlement with your agent. In addition, you can use the insurance carrier as the reason why you need to have all the other mechanisms in place.

Know all parts of the business. Learning all aspects of the business is incredibly useful. This does not mean you have to be an expert on everything. It simply means you have to have more than a superficial understanding of the duties and processes. Knowing every role makes you nearly impervious to having the wool pulled over your eyes. In addition, it also sends a message to the employees that you not only understand their role, but are able to check their work product and competence.

Manage cashflow. We already discussed having bank statements mailed to your home. You should also be making deposits on a daily basis. This process includes keeping a deposit ledger or log containing detailed information on the amount, the check number, patient receipts, etc.

Make sure that your employees know that you have a zero tolerance policy regarding embezzlement and theft.

Buy insurance. Discuss insurance that covers employee theft and embezzlement with your agent. In addition, you can use the insurance carrier as the reason why you need to have all the other mechanisms in place.

Adopt a zero tolerance policy. Make sure that your employees know that you have a zero tolerance policy regarding embezzlement and theft. Follow through with this policy by prosecuting any employee who steals. I made this mistake twice. I should have prosecuted both of the employees who embezzled funds. Don't threaten prosecution; don't promise not to prosecute if they return the money—that is extortion. In most states the court will require that the defendant pay restitution to the victim so you will get your money back.

Red Flags

1. Missing accounting records or gaps.
2. Discrepancies between deposits, receipts and bank statements.
3. Large petty cash funds that are not reconciled at the end of every shift.
4. Patient complaints about payment posting. "I paid a $50 co-pay but only received credit for $30."
5. Missing documents, invoices, receipts, etc.
6. Overdue notices from creditors, vendors, etc.
7. Employees insisting on doing a certain task or not wanting their work reviewed.
8. Lack of separation of duties.
9. Coming into the office late or not taking vacation days.
10. Forming "too close" relationships with accounting employees

As a leader, loyalty is a very admirable trait. However, do not let blind loyalty lull you into a false sense of security when dealing with disloyal and dishonest employees. Put policies and procedures in place so that you never have an, "et tu Brute" moment. ■

References

1. U.S. Chamber of Commerce
2. The Fair Credit Reporting Act requires this.