

Business Office Nightmares: Avoiding Theft

The modern Skilled Nursing Facility is in many ways a unique business operation. A 24-hour operation that takes care of our society's oldest and frailest with compassion, caring and integrity is a noble and challenging undertaking. Being the Nursing Home Administrator of a Skilled Nursing Facility is undoubtedly a stressful and rewarding, yet often thankless job.

There are definitely some nightmare scenarios for an Administrator from every side of the business. We are going to address just one of those here. We hope it helps you in some small way.

The sad truth is that when times are as tough as they have been for so many, more people are willing to "cross the line." With the economy the way it has been for so long, people who normally wouldn't even think of stealing are doing just that. We have been hearing more than ever of employees stealing from facilities. The money is being taken from resident trust accounts, petty cash accounts and more. Unfortunately, we have heard this from clients and colleagues alike.

We would like to share some ideas with you that we have seen help at several client facilities. As you can probably guess, they center on controls or checks and balances. How can you minimize the risk? There are several things you can do to prevent and detect problems. Who do you have to worry about? Anyone with access to accounts and cash can be a risk.

Resident Trust Accounts

As we all know, when the state walks in one of the first areas they look at in the business office is the resident trust. The risk with the resident trust is the abuse and misappropriation of resident funds. It is understandable why many affected facilities will simply quietly terminate the employee and move on when this happens, hoping to avoid attention and bad press.

If you can't implement anything else, you need to make sure you segregate duties. It is a standard accounting practice and safeguard to make sure that the person who receives and processes payments and distributions needs to be separate from the person who reconciles the accounts. If you get nothing else from all of this, **segregate the cash handling and posting duties from the reconciliation duties.**

What are your defenses? Know your residents, know their families, trust your staff, check their work and review the accounts.

The first thing you can do is to know your residents and families. The business office staff knows which families are attentive and which are not, so they know which accounts to try to manipulate first. The Administrator should also know the families and which ones are more susceptible to manipulation in order to keep an eye on these residents and their accounts. Be aware of risky transactions.

A good real-life example of an at-risk account is the husband of a resident who came into the facility every month to pay her \$3000-4000 bill in cash. There was never any problem at the facility where this gentleman came in every month, but the potential was definitely there. The Administrator knew he was coming in with the cash, but even more importantly he reviewed the accounts every month and the staff knew it. His vigilance effectively removed the temptation.

The accounts need to be reconciled monthly. The balances should be reviewed regularly as well. A report showing the monthly charges and balances of the past 2-3 months is a great help in spotting trends and unusual changes.

The administrator should regularly review receipts from charges against resident trust accounts. Several facilities have set an amount over which an approval and signature is required.

Statements should be provided to the resident or family regularly. We recommend monthly statements, but the quarterly basis that is mandated in many states is usually sufficient with good controls. We know of one instance in which the administrator had been told the statements were going out, but several were not sent for several months. A chance conversation with a family member led to the uncovering of dozens of sizeable fraudulent charges totaling several thousand dollars.

This may seem basic, but it needs to be said:

- The trust statements need to be clear and easy for the resident/family to understand.
- There should be no handwritten notes or explanations on the statement. If it isn't printed by your computer, that information is not in your system, so you have no paper trail.
- There should be both summary and detail pages.
- Always have information on disputing charges or contacting the business office or administrator on every statement.

If you are not using one of the resident trust services, we recommend you look into one. Even if you decide not to use one, the process of researching them can teach you quite a bit about how resident trust can, and perhaps should, work. Some possible benefits include:

- All of the resident's monthly income checks can be direct deposited to the facility having separated accounts and flexible reports. (SSI, VA, private pensions, etc).
- The resident liability portion of the direct deposited funds can be automatically separated and credited to a facility account.
- Resident liability payment data may be downloaded into a file that can be posted directly into your A/R system.
- Monthly account reconciliation reports can be provided to you.
- Internet access to reports for off-site monitoring may be available.

Theft of Resident/Private Payments

A staff member with A/R duties and little oversight can easily manipulate private payments.

A common scheme is to steal a private payment check made on a **Medicaid Pending** resident's behalf and leave the balance as Medicaid Pending. The resident or their family could be paying from day one, but the checks are being stolen. Since the Medicaid approval process can take a long time, and it is so common for the waiting period to be unpaid, the crafty A/R clerk can steal a few payments and then write it off later. Because private balances incurred while residents are Medicaid Pending are the source of the most numerous, and largest balance write-offs for most facilities, this is actually a good place to hide activity.

Again, the first thing to say here is **segregate** the A/R duties. The staff person who receives and posts the cash should not have access to the resident accounts and vice versa.

As we said with the Resident Trust accounts, the Administrator needs to review the monthly private pay statements. Check for anything irregular such as added charges, adjustments and handwritten notes on the statements. The rule is that if something is handwritten, then it is not anywhere in your system and you have no paper trail. Do not allow statements to be mailed out with handwritten notes on them.

The Administrator needs to be included in regular reviews of the aging report. We find it surprising how many larger organizations do not include the Administrator when the corporate office calls to review the aging with the Business Office Manager. He or she knows the families and might be able to pick up on any anomalies. If it seems strange that a family didn't pay who you were certain would, call them and see what they say about it.

Though a personal meeting is optimal, most Administrators don't have the time to meet with the resident/family upon Medicaid approval. You should use the approval as an opportunity to review their account history and their obligations from that point on with them. If there is a problem, it will show up then.

We have tried to cover what we have seen as the highest risk areas within the A/R side of the SNF business office. Of course there are other things to watch for in the A/R side, as well as the other functions. Unfortunately access to cash and checks can lead to temptation. Administrators and other

management personnel need to be vigilant in order to prevent and minimize the impact of the misuse of resident funds and outright theft from the facility.

What's the bottom line? Hire the best people you can. Train them as well as you can. Trust them and treat them like you trust them. Put good controls in place and be vigilant. Remember this doesn't happen everywhere and it doesn't need to occur at your facility. Make it as hard to get away with and as easy to detect as you can. Nobody needs to have to deal with this version of an Administrator's worst nightmare.

Thank you,

Your SNF Solutions Team

(407) 977-8878

www.snf-solutions.com

info@snf-solutions.com