PREVENTING FINANCIAL FRAUD:

What providers need to know about the laws governing financial exploitation and the controls needed to inhibit its growth

DID YOU KNOW?

- Only 1 in every 23 cases of elder Abuse, Neglect and Exploitation (ANE) is reported*
- Family, friends and caregivers are the perpetrators in 70 to 90% of all ANE**

- National Center on Elder Abuse and the National Long-Term Care Ombudsman Resource Center**, both of the Administration on Ageing, Washington, D.C.*

Whether due to the domestic financial recession or the deterioration of moral standards in today's society, just about every type of financial fraud is on the rise and the world of senior healthcare is not immune.

The U.S. Department of Justice recouped $3.8 billion last year in false claims, their second largest annual retrieval in history, bringing recoveries under the False Claims Act to $17 billion in the last four years alone, nearly half the total since the Act was amended in 1986.[1]

Similarly, financial exploitation is the fastest growing form of elder abuse today. As many as 1 in 10 elders experience abuse, neglect and/or exploitation (ANE), rising to 1 in 2 for individuals with dementia (see *Puzzle of Prevention*, Relias Learning, 2013). Elderly residents can be particularly vulnerable to financial exploitation due to cognitive decline, physical disability, recent loss of a partner or family member or when under the influence of an antipsychotic (*Partnering to Reduce*, Relias Learning, 2014).

"We're hearing from ombudsmen that the most prevalent form of financial exploitation tends to be misappropriation of funds, for example, family members or legal representatives that are supposed to be helping the elderly pay the home for their stay,"

1. *Department of Justice press release. http://www.justice.gov/opa/pr/2013/December/13-civ-1352.html*

said Lori Smetanka, Director, National LTC Ombudsman Resource Center (www.theconsumervoice.org). "But, the differences in oversight in long term care settings means that different types of financial exploitation may be easier to pull off. The type of financial exploitation depends on the type of long term care setting."

"We're hearing from ombudsmen that the most prevalent form of financial exploitation tends to be misappropriation of funds, for example, family members or legal representatives that are supposed to be helping the elderly pay the home for their stay."

- Lori Smetanka, Director, National LTC Ombudsman Resource Center

The rise in financial crimes against the elderly nursing home residents and those against facilities or the government have become a catalyst to compliance enforcement efforts like the establishment of the Health Care Fraud Prevention and Enforcement Action Team (HEAT), created by the U.S. Department of Health and Human Service (HHS) in 2009, or State Medicaid Fraud Control Units, established in 2012. Beyond these formal programs, surveyors have been trained to initiate a review of relevant facility protocols and procedures upon the identification of a potential fraud.

"Owners of nursing homes and home health agencies have to be more diligent when they're working in their business," Arlen S. Lasinsky, CPA, CFE, CFF, CTP, Director of Litigation/Forensic Services and Business Valuation at Deerfield, IL-based Frost, Ruttenberg & Rothblatt, P.C.. "Yes, they have people in position watching the store, but they have to be proactive and watch the store themselves. They have to be aware of warning signs that may exist."

"Owners of nursing homes and home healthcare agencies have to be aware that they can be a victim," said Lasinsky. "They need to be aware of that and not take anything for granted, thinking it can't happen to you."

- Arlen S. Lasinsky, CPA, CFE, CFF, CTP, Director of Litigation/ Forensic Services and Business Valuation at Deerfield, IL-based Frost, Ruttenberg & Rothblatt, P.C.

That is because the perpetrator is often close to home. According to the National Long-Term Care Ombudsman Resource Center, as many as 70 to 90% of perpetrators of crimes against elders are family, friends and caregivers. The same goes for crimes committed against senior care facilities and the federal government.

"The majority of those committing the frauds are trusted individuals. Typically, the higher the amount of fraud is committed by perpetrators higher up they are on the ladder of authority," said Lasinsky. "If you're the owner of a nursing home and I've been an employee there for 25 years, you know me like a book—even what shirt I'm going to wear on Mondays. So you trust me; you think I'm not going to steal from you. But, you might not know that I have a

certain habit or addiction that I don't have enough money to support. Trusted employees are seen as people that commit more fraud."

According to Lasinsky, perpetrators work slowly, gaining confidence in their fraud over time. "The perpetrators start out slow—maybe one transaction a month, and then next month they do two transactions, but by the end of their reign after many years, it seems that every transaction in the month belongs to them," said Lasinsky.

In order to meet the growing challenges of financial exploitation, providers across long term care (LTC), skilled nursing facilities (SNF) and home healthcare agencies must be versed in the most current laws and regulations governing fraudulent crimes. Armed with this knowledge, the provider can establish appropriate controls aimed at prevention.

A number of federal laws & regulations govern financial fraud and abuse as they apply to nursing homes, including:

1. The False Claims Act (FCA)
2. The Anti-Kickback Statute
3. The Exclusion Statute

Laws and Regulations

A number of federal laws and regulations govern financial fraud and abuse as they apply to nursing homes. For the limited purposes of this paper, these laws include: The False Claims Act (FCA), Section 6703(b)(3) of the Patient Protection and Affordable Care Act of 2010, the Anti-Kickback Statute and the Exclusion Statute. The Department of Justice, HHS and the Centers for Medicare and Medicaid (CMS) are charged with enforcing these laws.

The False Claims Act, first passed in 1863, protects the government from being overcharged or sold inferior goods or services. Breaches can result in fines up to three times the programs' loss, plus $11,000 per claim filed (each instance or service counts as an individual claim). Under the FCA, no specific intent to defraud is required. Instead, the FCA defines "knowing" of a fraudulent claim can even mean ignoring fraudulent acts or looking the other way. The FCA includes a whistleblower provision, or a "que tam," that allows a private individual to file a lawsuit on behalf of the United States and entitles them to up to a third of the money recovered alleging a false claim.

Section 6703(b)(3) of the Patient Protection and Affordable Care Act of 2010 requires LTC facilities that received at least $10,000 in federal funds during the preceding year to notify law enforcement officials with "any reasonable suspicion of a crime," which can include abuse, neglect or misappropriation of a resident's property. The report must be made no later than 24 hours after forming the suspicion (or within two hours in the case of serious bodily injury). LTC facilities are required "develop and maintain policies and procedures that ensure compliance," including posting a notice for employees specifying their right to file under the statute. The section also includes a provision stating that the facility "may not retaliate against an individual who lawfully reports a reasonable suspicion of a crime."

In some industries, it's acceptable to reward those who refer business through monetary payment or goods and services. However, remuneration (or providing a "kickback") with organizations that benefit from federal funding, is a crime. The **Anti-Kickback Statute** (AKS) is a criminal law that prohibits a knowing and willful payment of remuneration to induce the referral of federally funded businesses. Criminal penalties and administrative sanctions for violating the AKS can include fines (up to $50,000 per kickback, plus three times the amount of the remuneration), jail terms and exclusion from participation in federal healthcare programs, according to the Office of Inspector General (OIG).

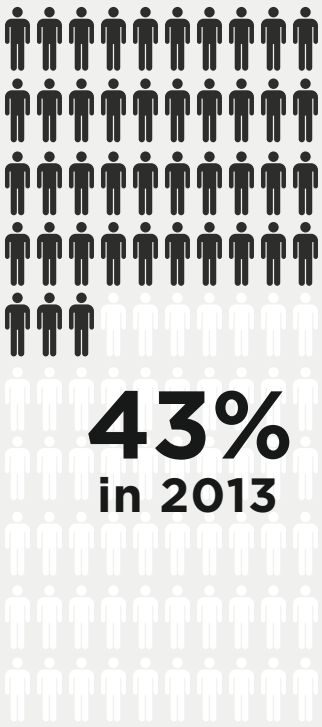
Finally, **The Exclusion Statute** excludes participation in all federal healthcare programs to individuals or entities that have been convicted of the following types of criminal offenses: Medi-care or Medicaid fraud, patient abuse or neglect, felony convictions of other healthcare related fraud, theft or financial misconduct, felony convictions for unlawful manufacture, distribution, prescription or dispensing of controlled substances.

For more information on these and more, visit: http://oig.hhs.gov/compliance/physician-education/01laws.asp.

ELECTRONIC IDENTITY THEFT

Healthcare identity theft is on the rise, accounting for 43% of all identity thefts reported in 2013, with more than half involving computer or other electronic breaches, according to the Identity Theft Resource Center (www.idtheftcenter.org).

"You can lock your door to protect physical records, and if someone steals them there's a limited distribution that can occur," said Pyles. "With electronic records, they can exist in an infinite number of places and can be stolen from anywhere in the world. The potential for this type of fraud is exponentially greater."



Effective 2009 under the Healthcare Insurance Portability and Accountability Act (HIPAA), all healthcare providers must notify patients if they believe their electronic health information was stolen, while the Department of Health and Human Services (HHS) must also be notified of electronic breaches involving 500 people or more. The latter is subject to pubic reporting on the department's Health Information Privacy site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html). When a violation of HIPAA's high tech security laws has occurred, a group practice, nursing home or hospital will be subject to fines and a compliance plan that will likely result in periodic monitoring and could lead to accusations of negligence under state law as well.

"Providers aren't doing enough to safeguard their systems. The HIPAA/HITECH rules are incredibly complex and conflicting," said Jim Pyles, Principal at Washington, D.C.-based health law and policy firm Powers, Pyles, Sutter & Verbille (www.ppsv.com). "Many providers don't have policies and procedures in place and have not done a risk analysis or training. All a patient has to do is find you didn't comply with one of these rules and sue you under the state negligence laws."

"Providers aren't doing enough to safeguard their systems. The HIPAA/HITECH rules are incredibly complex and conflicting."

Here are a few things providers can do to safeguard their residents' healthcare information, according to Pyles:

1. Make a good faith effort to be in compliance with all HIPAA standards. It may be difficult to be in complete compliance with all 80 HIPAA privacy and security rules, but it is possible to make a good faith effort. One of these rules requires the designation of a chief privacy office responsible for reviewing the list of standards like a checklist to make sure the facility or agency is either in compliance or taking steps towards compliance. Documenting this will provide a defense against negligence in the case of an alleged violation. Review the guidelines put out by the Office of Civil Rights to help. Visit http://www.hhs.gov/ocr/office/.
2. Buy cyber insurance. When doing so, make sure it does not have broad exemptions that would render it null and void. Companies will not insure those who have not made a good faith effort to be in compliance with HIPAA.
3. Policies and procedures. Conduct periodic training on policies and procedures to make sure all staff is up to date.
4. Review business associates and agreements. Make sure all business associates and agreements comply with HIPAA as well. This could be a medical billing vendor, pharmacy or a law firm that handles resident complaints. Any organizations you share electronic health information with must also comply.

SIX CONTROLS
a nursing home can implement to safeguard them and their residents

Controls

There are a number of controls a nursing home can put into place to assure proper policies and procedures to safeguard them and their residents from the threats of financial exploitation.

They are as follows:

1. Be an active owner

Knowing the nursing home's employees, customers, residents, families and vendors will help an owner recognize potential warning signs as they occur. When a staff member is living beyond their means or a reliable resident suddenly doesn't pay their rent, owners must recognize these warning signs and investigate further, and when necessary, take appropriate action immediately. "As an owner, you have to have your hand on the pulse of the business; you have to be able to know what's going on," said Lasinsky. "In a nursing home, maybe the owner needs to go online and look at their bank activity one day. No one needs to know you're doing it. You need to be hands-on to know what's really going on. Perpetrators are not counting on any deviation from the "norm" in daily activities."

2. Create a compliance program

An effective compliance program (see *Case for Compliance*, Relias Learning, 2011) will help any facility meet current regulations and requires: designating a corporate compliance officer to oversee all compliance activity; developing effective lines of communication with all entities, which often includes the set up of a compliance hotline for families and employees to voice complaints; developing a record keeping system to aid in accurately tracking care and billing; effective training and education (see #6); the establishment of disciplinary guidelines; exclusion checks for all employees, vendors and contractors; the development of an internal audit system and quality assurance committee. "Having a process for employee complaints is critical," said Jim Pyles, Principal at Washington, D.C.-based health law and policy firm Powers, Pyles, Sutter & Verbille (www.ppsv.com). "If they see something going on they don't think is right, have the organization's compliance officer investigate and

document everything. If there's a problem, own up to it and correct it. If a home received extra money, offer to return it using the self-disclosure process and let the employee know that you acted on their complaint. If the employee goes to the government after that, they will be prevented from a que tam recovery because the government will already have notice of the error."

3. Check controls

Fraudulent billing is prohibited by the False Claims Act and can apply to a number of different actions, including: the continued submission of claims for payment when not meeting the resident's needs, billing for services not actually provided, submitting claims for equipment or supplies that aren't medically necessary, upcoding reimbursement not clinically supported, duplicate billing, failure to identify and refund credit balances, forging physician or beneficiary signatures, filing false cost reports and more. Lasinsky suggests using treasury management or cash management tools offered to nursing homes and home health agencies by their banks such as payee positive pay to reduce check fraud, blocks and filters for electronic funds transfers (EFT's), mandating dual signatures on all checks over a certain dollar amount, maintaining separate accounts for disbursements and receipts and maintaining a locked vault for holding resident's cash that must be keyed by two or more employees to open.

4. Out of sight, out of mind

Home healthcare business owners should educate their staff members (see #6) as to what constitutes fraudulent billing and theft, including stealing from residents' homes. Similarly, they should educate family members and patients that when healthcare providers come into their home, valuables, including credit cards and bank information, should be hidden from sight.

5. Buy fraud insurance

Just like having fire insurance on a home, fraud insurance won't prevent the fraud itself, but can pay for partial or full damages when it occurs.

6. Training and education

The key to carrying out a facility's established policies and procedures is effective and ongoing training of nursing home staff. Online training modules like those from Relias Learning (www.reliaslearning.com) help nursing home and home health staff comply with their individual continuing education requirements while also providing training on current federal and state laws and regulations as they relate to potential healthcare fraud and the individual home's corporate compliance policies and procedures. "Facility administrators need to provide their staff with training about financial exploitation, residents' rights and facility responsibilities in protecting residents from abuse," said Amity Overall-Laib, Manager, Long-Term Care Ombudsman Program and Policy. "Establishing clearly-written policies and procedures about the role of the staff in protecting residents from financial exploitation and providing training will help staff understand what financial exploitation is, help them identify warning signs and know how to report it when they see something suspicious."

While these controls are critical to helping any nursing home comply with anti-fraud legislation, Lasinsky says there's no guarantee they will prevent it from happening in the first place.

"Internal controls are there to prevent the fraud and safeguard assets," said Lasinsky. "But, unfortunately, you can never have enough controls to stop the fraud where you will be totally protected. The best you can do is prevent it."

ADDITIONAL RESOURCES

- National Long Term Care Ombudsman Resource Center
  http://www.ltcombudsman.org/issues/elder-abuse-elder-justice
- Fact sheets for assisted living and nursing home residents
  http://www.theconsumervoice.org/node/1230
- Consumer Financial Protection Bureau, Office for Older Americans
  www.consumerfinance.gov/older-americans/
- Financial Education Program for Older Adults, FDIC
  www.fdic.gov/moneysmart
- National Center on Elder Abuse
  www.ncea.aoa.gov

Conclusion

Financial crimes both against nursing home residents, the facilities in which they live, home health agencies and the government are on the rise, with any number of perpetrators. Nursing homes must arm themselves with knowledge of current laws and regulations to keep their facilities and residents safe, while also making sure to safeguard their systems through the creation of policies, processes and controls.

"Owners of nursing homes and home healthcare agencies have to be aware that they can be a victim. They need to be aware of that and not take anything for granted, thinking it can't happen to you."

- Arlen S. Lasinsky, CPA, CFE, CFF, CTP, Director of Litigation/ Forensic Services and Business Valuation at Deerfield, IL-based Frost, Ruttenberg & Rothblatt, P.C.

"Owners of nursing homes and home healthcare agencies have to be aware that they can be a victim," said Lasinsky. "They need to be aware of that and not take anything for granted, thinking it can't happen to you. Fraud is a crime of opportunity and if you give someone the opportunity and they have a strong enough motivation, they will rationalize why their behavior is acceptable and they will steal."

About Relias Learning

Relias Learning is the premier provider of online education and communication for specialized industries. Our companies deliver the right level of training and expertise for employees working in specialized areas of health care, therapy, and the legal system. For more information, please visit www.reliaslearning.com.

RELIAS LEARNING