Long-Term Care Survey Alert

COMPLIANCE: Are Red Flags for Identity Theft on Your Risk Management Radar Screen?

Find out where these new requirements fit into the bigger picture.

If your facility hasn't complied with the so-called "red flag rules" to detect and prevent identity theft, it may be wide open to serious problems if someone steals a resident's personal financial information.

"The red flag rules apply to anyone who meets the regulation's definition of a creditor," which is an entity that provides services and charges for them later, says attorney **Joanne Lax,** with Dykema Gossett PLLC in Bloomfield Hills, Mich.

And that no doubt means your nursing facility.

What the rules require: Starting May 1, you need a written program to detect warning signs of identity theft, as well as "reasonable" policies and procedures to address and mitigate identity theft, according to the Federal Trade Commission, which oversees the rules. The facility also has to update the program periodically to reflect changes in risks related to identity theft, the FTC advises.

The consequences: The FTC can impose fines on entities found out of compliance with the red flag rules. As far as identity theft, a scenario where an unscrupulous staff person takes a resident's financial information or Social Security number for personal use could also raise survey compliance concerns, as it constitutes misappropriation of property,says Lax. And that "is a reportable aspect of resident abuse under the Medicare/Medicaid requirements of participation for long-term care facilities."

Identify Red Flags That Fit Your Facility

The federal regulations include an appendix that lists several possible "red flags," notes attorney **Scott Richardson,** with Bradley Arant Boult Cummings, in Nashville, Tenn."The regulations require that a committee be formed to consider a range of possible red flags and address how to detect and react" to them, he notes. But Richardson notes that "many facilities already have compliance teams, particularly HIPAA compliance teams, that are familiar with this area and can more easily take on this additional role."

Red flag these examples: Some potential red flags that might apply in a long-term care setting include getting mail back marked "undeliverable" when sent to a resident's given address, Richardson says. Or a resident or his representative may receive written correspondence from credit card companies or other financial institutions as if the resident had applied for consumer credit or a loan,when he hadn't. Unexplained charges on a resident's credit card can also be a potential sign that someone may have used the card number to order something online -- a scenario that has occurred in healthcare settings.

A red flag should also go up if someone's medical records don't match the person's history or what he or family members relay to you. Also look for instances where a returning patient's information doesn't match what you have on file from his previous admission, suggests Richardson.

Focus on All the Rules and Regs

Whether lack of compliance with the red flag rules ends up leaving surveyors seeing red remains to be seen, unless the Centers for Medicare & Medicaid Services issues guidance on the issue, says attorney **Joseph Bianculli,** in private practice in **Arlington, VA.**

But nursing home providers should keep in mind that the red flag requirements are only one part of an interrelated system of privacy laws and regulations, including HIPAA. Some states have specific anti-identify theft laws. In addition, state elder abuse laws may also weigh into the compliance equation.

That's why some legal experts advise healthcare organizations to focus on implementing an overall anti-identity theft effort. Such a program might include these strategies:

1. Always ask new admissions for a government-issued picture identification card to confirm who they are.

2. Compare the resident's identifying and medical information to what you have on file from Medicare or Medicaid or hospital records. In one case, a hospital detected identify theft by noting that a patient had a different blood type from the blood type in the original record, notes attorney **Robert Markette Jr.**, with Gilliland & Markette LLP in Indianapolis.

3. Set up a process to confirm guardianship status and HIPAA authorization in terms of identifying whom the facility can talk to about the patient, advises attorney **Cynthia Stamer** in Dallas. "Then the organization should continuously monitor it." This approach can head off a real-world scenario where a nursing home allowed a resident's neighbors to serve as her personal representatives when an attorney had actually been appointed for that purpose. And some of the resident's neighbors accessed her personal financial information -- and funds, Stamer relays.

4. Limit access to billing records. Some organizations keep these records separately, Stamer notes. Many facilities also authorize only certain personnel access to the information, Richardson points out.

5. Learn from past experiences with identity theft or attempted identity theft in the facility. The facility should make certain its red flag compliance plan addresses such instances to prevent them from happening again, stresses Richardson.