Eli's Hospice Insider

PRIVACY: 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 hospice thinks the so-called red flags rules to detect and address identity theft don't apply to it, take a closer look. And prepare to ramp up fast, if you haven't already, to comply with the new layer of privacy protection requirements, which go into effect on May 1.

The regulatory reality: The red flags requirements apply to creditors withcovered accounts, according to the Federal Trade Commission, which oversees the rules. "A creditor is any entity that regularly extends, renews, or continues credit," states the FTC. And a covered account involves multiple payments or transactions. The bottom line: The red flags requirements do apply to hospices,confirms attorney **Robert W.Markette Jr., CHC,** with Gilliland & Markette LLP in Indianapolis. "The rules address the issue related to hospice providing a service and billing Medicare or Medicaid later. That's considered to be 'credit.'" (Markette notes that a provider could be a creditor and not have a "covered account," which is an ongoing relationship. But that would be a rare instance where a provider delivers a service a single time, he says.)

What the rules require: Your hospice needs 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 FTC. The facility also has to update the program periodically to reflect changes in risks related to identity theft, the FTC advises. In addition, the board of directors or senior employees should manage the program, including "appropriate staff training" and oversight of service providers.

Nail Down the Red Flags for Your Hospice

The federal regulations include an appendix that lists several possible "red flags" signaling identity theft,notes attorney **Scott Richardson,**with Bradley Arant Boult Cummings in Nashville, Tenn.

The hospice has to identify which of the warnings apply to it and address how it will identify and react to those.

"A red flag for hospice would be information that doesn't match at intake," says Markette. "After the patient is admitted to hospice, red flags might involve information the hospice receives from a third party -- for example, someone else gets the EOBs," he adds.

Another red flag could be an instance where a hospice employee loses or has stolen a laptop with patient financial and medical information on it, he adds.

The red flags rules are hot right now due to their May 1 implementation date for healthcare providers, and the related press coverage.

But hospice and other providers should keep in mind that the red flags requirements are just another part of an interrelated system of privacy laws and regulations, including HIPAA.Some states have anti-identify theft laws and provisions. And elder abuse laws may also weigh into the compliance equation.

Watch out: If an organization has an employee who engages in identity theft, there's a good possibility that it would not only violate HIPAA and the red flag rules but also a number of other laws -- and there is imputed liability potentially, says **Cynthia Stamer,** an attorney in Dallas.

Best bet: Focus on implementing an overall anti-identity theft effort.Such a program might include the following strategies:

1. Ask the hospice patient to provide a government-issued picture ID when he goes on the benefit. And make sure there aren't any significant discrepancies between the medical history the patient and his family provide and what you find in the patient's medical record.

Markette is aware of one identity theft case in which a hospital identified that the patient had a different blood type from the blood type recorded in the original record."Medical identity theft in hospice is perhaps the worst," because it creates a false record that the person whose identity has been stolen has died.

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

3. Set up a process to confirm guardianship status and HIPAA authorization in terms of whom the organization can talk to about the patient, advises Stamer. "Then the organization should continuously monitor it." Stamer notes that hospices -- "due to the nature of care they provide -- often tend to assume that any-one who shows up is involved in the patient's care." Yet that assumption can have dire consequences if someone assumed to be a personal representative or part of the person's care helps himself to the person's funds or financial information.

4. Implement a policy requesting patients to lock up credit cards and valuables, suggests Stamer.This also helps protect employees from being accused by a forgetful family member or patient of stealing something.

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