Red Flags Rule - Guidance

Introduction
The purpose of the Red Flags Rule is to help detect the warning signs, or "Red Flags" of identity theft during day-to-day operations.

Enforcement
New legislation recently signed into law on December 18, 2010 now exempts healthcare providers from having to comply with the Red Flags Rule.

Identity Theft & Healthcare Providers
Although healthcare providers are now exempt, every health care organization and practice should review its billing and payment procedures to determine if additional precautions should be put in place to help detect the warning signs of identity theft. This guidance document helps outline steps that healthcare providers can take to help prevent identity theft for their patients.

Fraud Prevention Program
Your office may already have a fraud prevention or security program in place that you can use as a starting point.

Your program should:

1. Identify the kinds of red flags that are relevant to your practice;
2. Explain your process for detecting them;
3. Describe how you'll respond to red flags to prevent and mitigate identity theft; and
4. Spell out how you'll keep your program current.

Here are a few warning signs that may be relevant to health care providers:

- Suspicious documents. Has a new patient given you identification documents that look altered or forged? Is the photograph or physical description on the ID inconsistent with what the patient looks like? Did the patient give you other documentation inconsistent with what he or she has told you — for example, an inconsistent date of birth or a chronic medical condition not mentioned elsewhere?
- Suspicious personally identifying information. If a patient gives you information that doesn't match what you've learned from other sources, it may be a red flag of identity theft. For example, if the patient gives you a home address, birth date, or Social Security number that doesn't match information on file or from the insurer, fraud could be afoot.
- Suspicious activities. Is mail returned repeatedly as undeliverable, even though the patient still shows up for appointments? Does a patient complain about receiving a bill for a service that he or she didn't get? Is there an inconsistency between a physical examination or medical history

reported by the patient and the treatment records? These questionable activities may be red flags of identity theft.

- Notices from victims of identity theft, law enforcement authorities, insurers, or others suggesting possible identity theft. Have you received word about identity theft from another source? Cooperation is key. Heed warnings from others that identity theft may be ongoing.

Identity Theft Prevention Program Setup

Once you've identified the red flags that are relevant to your practice, your program should include the procedures you've put in place to detect them in your day-to-day operations. Your program also should describe how you plan to prevent and mitigate identity theft. How will you respond when you spot the red flags of identity theft? For example, if the patient provides a photo ID that appears forged or altered, will you request additional documentation? If you're notified that an identity thief has run up medical bills using another person's information, how will you ensure that the medical records are not commingled and that the debt is not charged to the victim? Of course, your response will vary depending on the circumstances and the need to accommodate other legal and ethical obligations — for example, laws and professional responsibilities regarding the provision of routine medical and emergency care services. Finally, your program must consider how you'll keep it current to address new risks and trends.

No matter how good your program looks on paper, the true test is how it works. Your program should be approved by your Board of Directors, or if your organization or practice doesn't have a Board, by a senior employee. The Board or senior employee may oversee the administration of the program, including approving any important changes, or designate a senior employee to take on these duties. Your program should include information about training your staff and provide a way for you to monitor the work of your service providers — for example, those who manage your patient billing or debt collection operations. The key is to make sure that all members of your staff are familiar with the Program and your new compliance procedures.

Attachment

RedFlags_forLowRiskBusinesses.pdf

References

Federal Trade Commission (FTC)
Red Flags Rule, from
http://www.ftc.gov/redflagsrule

This presentation and related material was prepared by tnREC, the HIT Regional Extension Center for Tennessee, under a contract with the Office of the National Coordinator for Health Information Technology (ONC), a federal agency of the Department of Health and Human Services (HHS). Contents do not necessarily reflect ONC policy. 90RC0026/01