

Red Flags Rule: Requirements for Health Care Providers September/October 2009 *Focal Point*

Medical identity theft occurs when a person seeks health care using someone else's name or insurance information. Victims may find their benefits have been used or encounter inaccuracies in their medical records. There may also be a high cost for health care providers due to unpaid bills.

The Red Flags Rule, enforced by the Federal Trade Commission as of November 1, 2009, requires many health care providers to develop a written plan (*Identity Theft Prevention Program*) to help detect, prevent and minimize the damage that could result from identity theft.

Who Must Comply

Every health care organization must review its billing and payment procedures to determine if the Red Flags Rule covers it. Status as a health care provider has no bearing on whether the law applies or not, but rather on whether a practice's activities fall within the law's definition of two key terms: **creditor** and **covered account**.

The law defines **creditor** to include:

- A practice that regularly defers payments for goods or services or arranges for the extension of credit. For example, you are a creditor if you regularly bill patients after the completion of services, including for the remainder of medical fees not reimbursed by insurance.
- Health care providers who regularly allow patients to set up payment plans after services have been rendered are considered creditors under the Rule.
- Health care providers are also deemed creditors if they help patients get credit from other sources, for example, distributing and processing applications for credit accounts tailored to the health care industry.

Health care providers are **not creditors**:

- If they require payment before or at the time of service. Simply accepting credit cards as a form of payment at the time of service does not make you a creditor under the Rule.
- If they accept only direct payment from Medicaid or similar programs where the patient has no responsibility for the fees.

Covered Account: a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft. The accounts you open and maintain for your patients are generally "covered accounts" under the law. If your practice is a "creditor" with "covered accounts," you must develop a written *Identity Theft Prevention Program* to identify and address the red flags that could indicate identity theft in those accounts.

Although there are no criminal penalties for failing to comply with the Rule, violators may be subject to financial penalties.

Creating an *Identity Theft Prevention Program*

Health care providers have the flexibility to implement a program that best suits the operation of their practice, as long as it conforms to the Rule's requirements. If there is already a fraud prevention or security program in place, it may be used as a starting point.

The program must:

- Identify the kinds of red flags that are relevant to the specific practice.
- Outline the process for detecting red flags within the daily operations.
- Describe its response to red flags to prevent and mitigate identity theft.
- Delineate a process for keeping the program current.

The program should include information about staff training and provide a way to monitor the work of service providers, for example, those who manage patient billing or debt collection operations.

The Federal Trade Commission has supplied a few warning signs that may be relevant to health care providers:

- **Suspicious documents** such as identification documents that look altered or forged, a photograph or physical description on the ID that is inconsistent with what the patient looks like, documentation inconsistent with what the patient has said. Under the Red Flags Rule, you may need to ask for additional information from that patient.
- **Suspicious personally identifying information** such as information that doesn't match what you've learned from other sources.
- **Suspicious activities** such as mail that is returned repeatedly as undeliverable, even though the patient still shows up for appointments; a patient complaining about receiving a bill for a service that he or she didn't get; 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. Heed warnings from others that identify theft may be taking place.

Resources

The FTC has published *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, a plain-language handbook on developing an Identity Theft Prevention Program. For a free copy of the Guide and for more information about compliance, visit ftc.gov/redflagsrule.

In addition, the FTC has released a fill-in-the-blank form for businesses and organizations at low risk for identity theft. The online form offers step-by-step instructions for creating your own written *Identity Theft Prevention Program*. You can fill it out online and print it. The do-it-yourself form is available at ftc.gov/redflagsrule.

If you have questions about the Rule, you may email RedFlags@ftc.gov.