MPC, Inc.

September 2009

Red Flags Rule

CELEBRATING 17 YEARS OF EXCELLENCE

MEDICAL PRACTICE CONSULTANTS, INC.

What Healthcare Providers need to know about complying with new requirements for fighting Identity Theft.

As many as nine million Americans have their identities stolen each year. The crime takes many forms. But when identity theft involves health care, the consequences can be particularly severe.

Medical identity theft happens when a person seeks health care using someone else's name or insurance information. A survey conducted by the Federal Trade Commission (FTC) found that close to 5% of identity theft victims have experienced some form of medical identity theft. Victims may find their benefits exhausted or face potentially life-threatening consequences due to inaccuracies in their medical records. The cost to health care providers — left with unpaid bills racked up by scam artists — can be staggering, too.

The Red Flags Rule, a law the FTC will begin to enforce on August 1, 2009, **(as of August 3rd, it has been postponed until November 1, 2009)** requires certain businesses and organizations — including many doctors' offices, hospitals, and other health care providers — to develop a written program to spot the warning signs — or "red flags" — of identity theft. Is your practice covered by the Red Flags Rule? If so, have you developed your Identity Theft Prevention Program to detect, prevent, and minimize the damage that could result from identity theft?

Who Must Comply

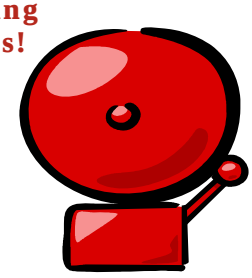
Every health care organization and practice must review its billing and payment procedures to determine if it's covered by the Red Flags Rule. Whether the law applies to you isn't based on your status as a health care provider, but rather on whether your activities fall within the law's definition of two key terms: "creditor" and "covered account."

Health care providers may be subject to the Rule if they are "creditors." Although you may not think of your practice as a "creditor" in the traditional sense of a bank or Mortgage Company, the law defines "creditor" to include any entity 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. Similarly, health care providers who regularly allow patients to set up payment plans after services have been rendered are creditors under the Rule. Health care providers are also considered creditors if they help patients get credit from other sources — for example, if they distribute and process applications for credit accounts tailored to the health care industry.

On the other hand, health care providers who require payment before or at the time of service are not creditors under the Red Flags Rule. In addition, if you accept only direct payment from Medicaid or similar programs where the patient has no responsibility for the fees, you are not a creditor. Simply accepting credit cards as a form of payment at the time of service does not make you a creditor under the Rule.

The second key term — "covered account" — is defined as 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 organization or 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.

Back to learning and implementing new regulations!



MEDICAL PRACTICE CONSULTANTS, INC.
Renee M. Brown, President
50 Penn Place
1900 NW Expressway, Suite 625
Oklahoma City, Oklahoma 73118
(405/848-8558)

Spotting Red Flags

The Red Flags Rule gives health care providers flexibility to implement a program that best suits the operation of their organization or practice, as long as it conforms to the Rule's requirements. Your office may already have a fraud prevention or security program in place that you can use as a starting point.

If you're covered by the Rule, your program must:

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.

What red flags signal identity theft? There's no standard checklist. Supplement A to the Red Flags Rule — available at ftc.gov/redflagsrule — sets out some examples, but 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? Under the Red Flags Rule, you may need to ask for additional information from that patient.

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.

Setting Up Your Identity Theft Prevention Program

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. According to the Red Flags Rule, your program must 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 Rule and your new compliance procedures.

What's At Stake

Although there are no criminal penalties for failing to comply with the Rule, violators may be subject to financial penalties. But even more important, compliance with the Red Flags Rule assures your patients that you're doing your part to fight identity theft.

Looking for more information about the Red Flags Rule? 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 *http://www.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 *http://www.ftc.gov/redflagsrule*. Questions about the Rule? Email RedFlags@ftc.gov.

"An education isn't how much you have committed to memory, or even how much you know. It's being able to differentiate between what you do know and what you don't."

By Anatole France (1844-1924)