

THE FTC'S NEW "RED FLAG" RULES: DO THEY APPLY TO YOUR MEDICAL PRACTICE?

By: Heather R. Baldwin Vlasuk
Walter & Haverfield LLP
Cleveland, Ohio

On November 1, 2009, the Federal Trade Commission (FTC) will begin enforcing its so-called "Red Flag Rules," which require creditors to create and implement a written Identity Theft Prevention Program. The Rules went into effect on January 1, 2008, but enforcement of the Rules have been postponed to allow entities time to come into compliance with the regulations. The goal of the Rules is to attempt to minimize the incidents and impact of identity theft.

In creating these Rules, as an expansion to the existing Fair And Accurate Credit Transaction Act (FACTA), the federal government continues to recognize that identity theft can have a real and lasting impact on its victims. In the realm of healthcare, when an individual's identity is stolen, more than financial repercussions can occur. For example, false and inaccurate medical histories may be created, leading to inappropriate treatment and/or denial of health insurance claims or coverage.

Despite the admirable goal of the Rules, there has been some push in the medical community to seek an exemption from the Rules for healthcare providers. However, at the moment, the FTC has taken a firm stance that there is no industry-based exemption to the Red Flag Rules. Additionally, the FTC has clarified that HIPAA compliance and maintenance of ethical obligations to protect patient confidentiality do not relieve healthcare providers from compliance with the Red Flag Rules.

Because of the broad definition of "creditor" under the Rules, many healthcare providers, even those with small practices who do not seem to extend credit in the traditional sense, may still be subject to the Rules. Consequently, the enforcement date leaves many businesses scrambling to find out what needs to be done to come into compliance with the Rules.

Are You Subject To The Rules?

The first step in faring your way through the Red Flag Rules is to determine if you extend "credit" for accounts used primarily for personal, family or household services; i.e., patient accounts for medical care. "Credit" is defined basically as deferring payment for products or services. But what does this mean for healthcare providers? In short, payment plans constitute deferral of payment and are, therefore, an extension of credit. And, according to the FTC, even deferring payment to allow a claim to be submitted to the patient's insurance and billing the patient later constitutes extending credit, regardless of whether it is done as a courtesy to the patient or because it is required under contractual or state law. Therefore, if your business utilizes payment plans or postpones payment in order to submit claims to insurance, it is likely that you must comply with the new Rules.

What Now?

Fortunately, the Red Flag Rules, and indeed the FTC, recognize that businesses, including medical practices, are not uniform. The Rules allow leeway for businesses to design and implement an identity theft protection program that is appropriate to its size, complexity, and the nature of the business. In fact, the FTC has stated that it expects that businesses for which the risks of identity theft are “minimal or non-existent will have a very low burden under the Rules.” For example, a small medical practice with a well-known, limited patient base might have a lower risk of identity theft, and thus may adopt a more limited identity theft program than a clinic in a metropolitan setting that has a high volume of customers that sees a high volume of new patients.

However, regardless of the size of your medical practice, basic steps need to be taken in order to comply with the Rules. You must assess the risk for identity theft in your practice and create a written program that identifies warning signs of identity theft (so-called “red flags”), implements a procedure to detect the “red flags,” sets forth a procedure to respond to “red flags” when they occur, and establishes a schedule for periodic review of the program, updates, and personnel training.

Creating A Program

As previously discussed, an Identity Theft Prevention Program may be tailored to each healthcare provider based on its size, nature and scope of the practice. Generally, the Program will identify “red flags” of identity theft that may arise. Examples of “red flags” are:

- Alerts, notifications, other warnings received from consumer reporting agencies;
- Presentation of suspicious documents (e.g., obvious forgeries or physical descriptions or photos not matching the person providing the document);
- Suspicious personally identifiable information (e.g., fictitious addresses, inconsistent personal information; lack of correlation between SSN range and date of birth);
- Other suspicious activity on the account (e.g., suspicious change of address); and
- Notices from patients, victims of identity theft, law enforcement, or other persons regarding the possibility of identity theft in connection with the account.

Once the “red flags” of identity theft are identified, the Program must set forth a plan to detect the “red flags.” For example, a detection method may consist of checking photo identification at the time services are sought to ensure that individuals seeking medical treatment are who they represent themselves to be. Another approach may be to add a photo of the individual to the medical file upon the first visit and to compare such

photo against subsequent persons seeking service under that name. Also, if patients provide their social security number, there are simple rules-of-thumb to detect SSNs that are invalid on their face based on the numbers composing the SSN. Larger practices may want to subscribe to commercial services that can screen for SSN validity.

Next, the Program must set forth an appropriate response procedure for when a “red flag” has been detected, so that the identify theft is prevented and/or its impact is mitigated. One starting point may be to ask the patient to explain any discrepancies between conflicting personal information, such as when the address on the driver’s license does not match the address given by the patient. Also, if it appears that a person seeking treatment is not the current patient for whom the personally identifying information corresponds, an appropriate response may be to notify the original patient and to refrain from commingling the medical information for the two individuals. Other responses may include changing security codes for external access to patient accounts and medical records, declining to open an account or closing and renumbering an existing account, and actively monitoring or notating specific accounts if the healthcare provider is notified by a patient of the potential for identity theft. Additionally, the Program should provide that collection on the account be stopped, if identify theft has actually occurred.

The Program should also provide for all non-reconciled “red flags” to be reported to a specific person, such as the chief practitioner, who would have the responsibility to take further action appropriate in the situation, such as thoroughly reviewing the circumstances and notifying law enforcement authorities if there is credible evidence that identity theft has occurred.

Implementing The Program

After the Identity Theft Prevention Program is created, it must be approved, implemented, and administered. Under the Rules, the Program must be formally approved by the entity’s board of directors. If there is no board, the approval should be made by the highest executive authority (i.e., the entity’s president, management committee, or owner of a sole proprietorship). Also, the board of directors, an appropriate committee of the board, or a designated member of senior management must oversee, implement and administer the Identity Theft Prevention Program.

Furthermore, appropriate workplace training must occur, such as providing general training for all staff members and more extensive training on the Program for staff members charged with patient registration. It is recommended that the Identity Theft Prevention Program be made part of the initial training of all new staff members as well as part of annual training. Records that such training occurred should be kept by the employer.

The Program must also be periodically reviewed and updated based on the business’ experience in encountering identity theft and based upon any changes to the size, nature and scope of practice. At least annually, staff should provide a written report to the board or designated senior management regarding significant incidents involving

“red flags” and management’s response, the effectiveness of the policy and procedures, and recommendations for change.

If a practice involves service provider arrangements allowing third-party access to patient accounts, such as outsourced billing, the healthcare provider must take some steps to ensure that the third-party complies with its own identify theft protection program. This oversight of service provider arrangements may be accomplished through mandating such requirements in service provider agreements.

Again, keep in mind that Identity Theft Prevention Programs under the new Red Flag Rules can and should be tailored to your practices’ specific size, complexity and nature. Solo practitioners with minimal staff do not need to create the same type of program as would be required of hospitals or large clinics. What is required, however, is that healthcare providers follow each step listed above to create, implement, oversee, and periodically update an appropriate Program. Of course, if you should have any concerns as to whether the policy you are creating brings your practice into full compliance with the Rules, you should seek the advice of legal counsel.

To recap the Red Flag Rules

Step 1: Assess whether your entity is subject to the regulation.

A healthcare provider is subject to the Red Flag Rules if the provider extends credit and maintains “covered accounts.” Credit includes deferring payment for services to a later date. A “covered account” is defined as an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Patient accounts are accounts for personal purposes and if multiple payments can be made on the account, the FTC considers it a “covered account” under the Red Flag Rules.

Step 2: Draft and Implement an Identity Theft Protection Program

Entities subject to the Red Flag Rules must design and implement an identity theft protection program which does the following:

- 1.) *Identifies Covered Accounts.*
- 2.) *Identifies Red Flags* - “Red flags” are warning signs of identity theft. Some types of “red flags” are:
 - Alerts, notifications, other warning received from consumer reporting agencies;
 - Presentation of suspicious documents (e.g., obvious forgeries or physical descriptions or photos not matching the person providing the document);

- Suspicious personally identifiable information (e.g., fictitious addresses, inconsistent personal information; lack of correlation between SSN range and date of birth); and
 - Other suspicious activity on the account (e.g., suspicious change of address).
- 3.) *Detects Red Flags* – the Program must contain reasonable approaches to detecting the identified “red flags.” One example would be instituting a policy to verify the patient’s identity at time of registration.
- 4.) *Responds to Red Flags* – the Program must set forth a process to prevent and mitigate the damaging effects of identity theft through appropriate responses to “red flags.” Examples of appropriate responses may be:
- monitoring covered accounts for evidence of identity theft;
 - contacting the patient or account holder;
 - changing security codes for external access to patient accounts and medical records;
 - declining to open an account or closing an existing account; and
 - notifying law enforcement.
- 5.) *Provides for administration of the program, periodic updates, and employee training.*

Step 3: Approve the Program

The entity’s board of directors or other appropriate committee thereof must approve the Program. Also, either the board of directors or a senior level employee must be involved in the oversight, development, implementation, and administration of the program.

Further Information

Once again, it is recommended that entities consult with legal counsel to determine if they are subject to the Red Flag Rules and to create and implement a program in compliance with the Rules; therefore, physicians are encouraged to contact their legal counsel regarding this issue. **If you have questions regarding the “Red Flag Rules,” please feel free to contact Heather R. Baldwin Vlasuk or Amy Leopard at the law firm of Walter & Haverfield, LLP at (216) 781-1212.**