Federal Trade Commission’s “Red Flags Rules”

What are the Red Flags Rules?
The Red Flags Rules were developed pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under the Rules, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. At the request of several Members of Congress, the Federal Trade Commission is further delaying enforcement of the “Red Flags” Rule through December 31, 2010, while Congress considers legislation that would affect the scope of entities covered by the Rule.

Who is Covered Under the Rules?
The Red Flags Rules apply broadly to all financial institutions and “creditors” that maintain “covered accounts.” An entity must first determine if it qualifies as a “creditor” under the Rules. A “creditor” is defined as any person or entity that:

- Regularly extends, renews, or continues credit (e.g., allowing a patient to pay after any care is rendered instead of payment in full in advance is considered the extension of credit);
- Regularly arranges for the extension, renewal, or continuation of credit; or
- Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit for a covered account. Any health care provider that defers payment (even under a “net-30 days” arrangement) will be considered a creditor under the Rules. If a health care provider determines that it qualifies as a creditor, it must then determine if it offers or maintains one or more “covered accounts.” There are two categories of “covered accounts” under the Rules:
  - A consumer account that is maintained primarily for personal, family, or householder purposes and that involves or is designed to permit multiple payments or transactions. Most patient accounts qualify as such consumer accounts.


• Any other account that the creditor offers or maintains and that involves a foreseeable risk of identity theft.³

**Do the Rules Apply to Health Care Providers, including Hospices?**

Based on FTC guidance, health care providers, including hospices, can and usually do qualify as “creditors” subject to the Rules. In particular, health care providers who regularly bill consumers after services are completed may qualify as “creditors” who maintain “covered accounts,” since they are entering into agreements to provide services on a regular basis and accepting deferred payments. Similarly, health care providers who accept insurance are considered creditors if the consumer is ultimately responsible for any medical fees since in such instances the health care provider is deferring the consumer’s payment of his or her share of the fees, pending the insurer’s determination and payment of their obligation. However, a service arrangement between a provider, an insurance plan, and a patient, where the individual patient has no personal responsibility for payment (including no co-payment) likely would not trigger a creditor relationship under the Rules. Moreover, a provider’s mere acceptance of credit cards alone does not qualify it as a creditor under the Rules.

**What is My Hospice Required to Do if it is Covered under the Rules?**

Health care providers and related entities that qualify as creditors and maintain covered accounts are required to develop a written Identity Theft Prevention Program (the “Program”). Resources for developing a Program are provided below. The Program must be designed to detect, prevent, and mitigate identity theft in connection with new or existing covered accounts.⁴ In particular, the Program must contain reasonable policies and procedures to:

- Identify and detect identity theft “red flags” that may be encountered in day-today operations;
- To respond appropriately to any “red flags” that are detected; and
- To ensure that the Program is periodically updated to reflect any changes in risk. Red flags are patterns, practices or specific activities that indicate the possible existence of identity theft.⁵ In the health care context, the FTC has indicated this may include such things as:

---


⁴ 16 C.F.R. § 681.2(d)

An individual demanding services or access to health information with unusual frequency or urgency;

- Providing personal identifying information that is inconsistent with information on file;

- A complaint or question from an individual based on their receipt of a bill from another person or entity for a service they did not receive; or

- A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

There are also additional administrative requirements imposed on covered entities by the Rules. A covered health care provider’s Board of Directors or senior management must assume responsibility for the development and administration of the Program. This includes:

- Approving the initial written Program;
- Maintaining oversight over the Program;
- Implementing training; and
- Exercising oversight over contracted service providers used in connection with covered accounts.

Health care providers and entities are given flexibility in designing a Program. The exact structure of the Program can vary based on a provider’s business needs, as well as the size and complexity of the provider’s business and their risk of identity theft. Health care providers and entities are also allowed to build off of existing identity theft prevention programs.

**Frequently Asked Questions**

**As a health care provider I occasionally accept late payments, does this automatically make me a “creditor” under the Red Flags Rules?**

**Answer:** No. The determination of creditor status depends on when payments are regularly and actually due, not on isolated cases that are the exception to the provider’s general rule or policy. This requires a facts and circumstances analysis. For example, if your business has a policy that payment is due at the time of services, but it provides a “grace period” before late fees are charged, it is unlikely that this grace period policy would make your business a creditor since payment is actually due at the time of service. However, if your business regularly allows for late payments or has a policy that formalizes the extension of credit (i.e., payment is not due at time of service for certain customers), then your business probably is a creditor based on that policy. Additionally, health care providers who accept insurance are considered creditors if the consumer is ultimately responsible for any medical fees since in such instances the health care provider is deferring the consumer’s payment of his or share of the fees by billing the insurance carrier first.
Does my business have to implement a Program if we already have data security policies and comply with other federal health privacy and security requirements, such as HIPAA?

Answer: The Red Flags Rules are not data security rules. The Rules are designed to target instances when an identity thief already has someone’s personal data or health information and is attempting to use it. Data security rules typically aim to prevent an initial theft of personal information, but do not necessarily address ways to respond to an identity thief’s attempt to use someone else’s personal information. In this respect, the Rules are designed to supplement data security measures that your business may already have in place. This includes HIPAA’s privacy and security requirements. The Rules help in preventing or mitigating the misuse of personal health information that may have been obtained as a result of medical identity theft.

If I determine that I am a creditor under the Rules, what types of accounts does my Program have to cover?

Answer: The Rules require that creditors implement a written Program that addresses all “covered accounts.” Therefore, even if a particular account does not trigger creditor status, if it qualifies as a covered account then it must be addressed in the Program.

What if my business meets the definition of creditor and offers or maintains covered accounts, but we believe we are at a low risk of identity theft?

Answer: All businesses that qualify as creditors and that offer or maintain covered accounts are required to implement a Program. However, the Rules are risk-based. Therefore, if your business only has a low risk of identity theft, it has a low burden under the Rules and can have a less complex Program. For example, if a health care provider is at low risk for identity theft, an appropriate program might include verifying photo identification at the time services are rendered and having procedures in place to respond to complaints of identity theft. For entities that have a low risk of identity theft, the FTC is also releasing a template to help the entities comply with the Rules. When this template is available, NHPCO will make it available on its website.

What are the penalties for non-compliance?

Answer: Although there are no criminal penalties, covered health care providers and other entities who do not implement a proper Program may be subject to civil monetary penalties. The FTC recently granted a three month delay of enforcement of the Rules for all entities under its jurisdiction. The new enforcement date is August 1, 2009.
Red Flag Rule Resources:

Supplement to the Rules. A supplement to the Red Flags Rules provides twenty-six examples of red flags, which covered entities must consider when formulating a Program. Covered health care providers should review the examples and, when relevant, incorporate them into their Programs. They must also adopt other reasonable policies and procedures to meet the specific requirements of the Rules.

How-To Guide - "How-To Guide for Businesses" has been published by the FTC and is available for download.

Federal Trade Commission press releases

- April 2009
- October 8, 2008
- June 2008

Articles of interest:

- FTC Delays Enforcement of FACT Act Red Flags Rules - Press Room Hogan & Hartson (October 2008)
- What the FTC's Identity Theft Rules (a.k.a. The Red Flags Rules) Mean for Health Care and Senior Housing Providers - Headlines in Health Law (January 2009)
- Red Flags Rules: Obligations of Health Care Providers – Arent Fox (May 2009)