

RATH YOUNG PIGNATELLI

National Impact. Uniquely New Hampshire.

Health Care Providers' Obligations under the FTC's Red Flag Rules

What Health Care Providers Need to Know

Hospitals, physicians and other health care providers should know that they may be subject to the Federal Trade Commission's Red Flag Rules. The Red Flag Rules apply to financial institutions and "creditors," and are designed to protect against identity theft. The original date for compliance with the Red Flag Rules was November 1, 2008 but the FTC has recently announced a six-month delay.

The FTC has interpreted these rules as applying in the health care sector, where medical identity theft is a real concern. Medical identity theft occurs when someone uses another person's name and sometimes other parts of their identity, such as insurance information or Social Security Number, without the victim's knowledge or consent, to obtain medical services or goods..

When is a Health Care Provider Covered by the Red Flag Rules?

A health care provider is covered by the Red Flag rules if it is a "creditor" that offers or maintains "covered accounts."

A "creditor" is any entity that regularly accepts deferred payment for goods and services. Health care providers that provide services to patients and regularly permit patients to pay for such services over time through a payment plan would likely be considered "creditors."

An "account" means a continuous relationship established by a person with a creditor to obtain a product or service. An ongoing provider/patient relationship with a provider who is a "creditor" would be an account.

A "covered account" means an account designed to permit multiple payments or transactions, as well as any other account for which there is a reasonably foreseeable risk of identity theft. Patient medical and billing records contain the patient's name, address, and other personal identifying and financial information, and are likely "covered accounts."

Providers' Ordinary Billing and Collection Practices & the Red Flag Rules

There is some uncertainty as to whether ordinary billing and collection practices will make hospitals, physicians and other providers “creditors” and thus subject to the Red Flag Rules.

For example, according to the American Medical Association, some FTC staff attorneys have interpreted the term “creditor” too broadly, viewing a physician as a “creditor” if he or she does not demand payment in full at the time services are rendered, and instead bills the patient after the services are rendered. Apparently some FTC attorneys have said that a physician is a “creditor” if he or she agrees to bill the patient’s health insurance first, but holds the patient ultimately responsible for amounts not covered by the insurance, such as co-pays, deductibles, and services not covered by insurance.

The AMA strongly disagrees with this position, and sent a letter to the FTC explaining why most physician practices should not be considered “creditors.” The AMA’s letter requested that the FTC withhold any plans to apply the Red Flag Rules to physicians until the matter is resolved.

Six-Month Delay in Enforcement

The original deadline for compliance with the Red Flag Rules was November 1, 2008. However, the FTC recently announced that it will suspend enforcement of the Red Flag Rules until May 1, 2009, in order to give those entities that may not have been aware that they were subject to the Rules—such as health care providers—time to establish appropriate identity theft programs.

It is not clear whether the FTC will respond to the AMA’s specific concerns before the new deadline.

Requirements of Red Flag Rules

The Red Flag Rules require a creditor that offers or maintains “covered accounts” to develop and implement a written identity theft prevention program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Red Flag Rules provide considerable flexibility, allowing entities to establish programs that are appropriate given their size and complexity and the nature and scope of their activities.

The program must include reasonable policies and procedures to:

- Identify relevant red flags. (A “red flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft.)
- Detect red flags.
- Respond appropriately to any red flags that are detected.

The program must be approved initially by the entity's board of directors (or an appropriate committee of the board), and must be updated periodically. The board or committee must remain involved in the program's oversight and administration. The entity must provide appropriate training for staff.

Guidelines for Developing Policies and Procedures

It should not be overly burdensome for providers who are subject to the Red Flag Rules to develop appropriate policies and procedures, particularly in view of the flexible approach taken by the Rules. Also, because there is some overlap between the Red Flag Rules and HIPAA, many health care providers may already have some of the requisite policies in place.

Resources are available. An appendix to the Red Flag Rules contains useful guidelines on identity theft detection, prevention, and mitigation. A supplement to the guidelines lists sample red flags. As well, the World Privacy Forum has published a helpful paper that explains the application of the Red Flag Rules to health care providers and provides good practical advice. For example, the paper lists red flags that might arise in a health care context, including:

- A complaint or question from a patient based on the patient's receipt of:
 - a bill for another individual;
 - a bill for a product or service that the patient denies receiving;
 - a bill from a health care provider that the patient never patronized;
 - a notice of insurance benefits for health services never received.
- Records showing medical treatment that is inconsistent with the physical examination or a medical history as reported by the patient.
- A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.

Helpful Links

For the Red Flag Rules and a complete discussion of their requirements, please [click here](#) to see 72 Federal Register 63718, or go to 16 CFR Part 681 to review the text of the FTC rules.

For the World Privacy Forum paper "Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers," please [click here](#).

For the AMA's letter to the FTC, please [click here](#).

For the FTC's October 22, 2008 press release announcing a six-month delay in enforcement of the Red Flag Rules, please [click here](#).

For more details, please contact Lucy Hodder at 603.410.4340 or lch@rathlaw.com, or Barbara Greenwood at 603.410.4306 or bjg@rathlaw.com.