

Federal Trade Commission's "Red Flags" rule

As part of the Federal Trade Commission's (FTC's) implementation of the Fair and Accurate Credit Transactions (FACT) Act of 2003, medical providers may need to comply with the "Red Flags" rule, which requires "creditors" to establish a program to prevent identity theft in their practices. The program, as discussed in more detail below, must incorporate Red Flags – that is, indicators of a possible risk of identity theft. While the rule was originally scheduled to go into effect on Nov. 1, 2008, advocacy efforts by the Medical Group Management Association (MGMA) and other medical associations resulted in a six-month delay in enforcement until May 1, 2009. MGMA still has concerns about the application of this rule to health care providers, including the late notification by the FTC that providers are considered "creditors." As a result, the health care community was not able to provide meaningful comments to the agency on the rule, as would normally be the case in the rulemaking process. We are still engaged in advocacy efforts on this issue but have provided this information to assist you in planning for the May 1 compliance date. In a Feb. 4 correspondence to MGMA and others in the medical provider community, the FTC maintains its position that certain health care providers are creditors.

Who is a creditor?

The Red Flags rule (<http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf>) defines a creditor as "any person who regularly extends, renews, or continues credit; any person who 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." The FTC interprets this to include a medical provider if the provider does not regularly demand payment in full for services or supplies at the time of service. This includes, for example, a provider who bills a patient's insurance company before requesting payment in full from the patient. In its most recent correspondence, the FTC reinforced this point by stating:

When a physician submits a claim to an insurance carrier first and then bills any remaining unpaid amounts to the patient – whether she does so as a courtesy to the patient or because she is required to do so as a matter of contractual or state law – the physician is deferring the consumer's payment of his or her share of the claim (i.e., the physician is billing the patient after having provided the patient with medical services).

The FTC considers a physician who engages in this type of arrangement to be a creditor for purposes of the Red Flags rule.

What are covered accounts?

Once an entity determines that it is a creditor, the next question is whether it maintains “covered accounts.” As defined in the regulations, covered “accounts” are accounts that permit multiple payments or transactions and those that pose a reasonably foreseeable risk to customers or to the safety and soundness of medical practices from identity theft, including financial, operational, compliance, reputation or litigation risks. The FTC considers patient billing records to be “covered accounts.”

What does the Red Flags rule require?

If a practice determines it qualifies as a creditor that maintains covered accounts, the Red Flags rule applies. The practice will be required to develop an identity-theft prevention program that contains "reasonable policies and procedures" (which may incorporate existing policies and procedures) to achieve the following goals:

- 1. Identify relevant indicators of a possible risk of identity theft (“Red Flags”)**
- 2. Detect Red Flags**
- 3. Prevent and mitigate identity theft**
- 4. Update the identity theft prevention program**

The following guidance is based on the FTC’s publications and communications regarding the Red Flags rule. Note also that the FTC, in its recent correspondence to the medical community, stated that, due to the risk-based nature of the requirements, it did not believe the rule would impose significant burdens on most providers. It gave examples of a low-risk practice (a small practice with a limited, well-known patient base) and a high-risk practice (a clinic in a large metropolitan area that treats a high volume of patients). It stated that in low-risk practices, an appropriate program might involve checking photo identification and having policies to deal with the theft of a patient’s identity (including not trying to collect the debt from the patient and separating the medical records of the real patient from those of the identity thief).

1. Identifying relevant indicators of a possible risk of identity theft (“Red Flags”)

In identifying Red Flags, a practice should consider:

- The types of covered accounts it offers or maintains
- The methods it provides to open its covered accounts (in the case of health care providers, this could include the intake procedure for new patients)
- The methods it provides to access its covered accounts and
- Its previous experiences with identity theft

Red flags can come from a number of sources, including:

- Incidents of identity theft that the practice has experienced

- Methods of identity theft that the practice has identified that reflect changes in identity theft risks
- Applicable supervisory guidance

The following categories of Red Flags are offered as guidance by the FTC in its rule:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
- The presentation of suspicious documents:
 - Documents provided for identification appear to have been altered or forged
 - The photograph or physical description on the identification is not consistent with the appearance of the patient presenting the identification
 - Other information on the identification is not consistent with information provided by the patient
 - Other information on the identification is not consistent with readily accessible information that is on file with the practice
 - An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled
- The presentation of suspicious personal identifying information, such as a suspicious address change:
 - Personal identifying information provided is inconsistent when compared against external information sources used by the practice, for example:
 - The address does not match any address in a consumer report or
 - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File
 - Personal identifying information provided by the patient is not consistent with other personal identifying information provided by the patient. For example, there is a lack of correlation between the SSN range and date of birth
 - Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the practice. For example:
 - The address on an application is the same as the address provided on a fraudulent application or
 - The phone number on an application is the same as the number provided on a fraudulent application
 - Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the practice. For example:
 - The address on an application is fictitious, a mail drop, or a prison or
 - The phone number is invalid, or is associated with a pager or answering service
 - The SSN provided is the same as that submitted by other persons opening an account or other patients

- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other patients
- The patient fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- Personal identifying information provided is not consistent with personal identifying information that is on file with the practice
- If the practice uses challenge questions to identify patients, the patient cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report
- The unusual use of, or other suspicious activity related to, a covered account:
 - Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account
 - The practice is notified that the patient is not receiving paper account statements
 - The practice is notified of unauthorized charges or transactions in connection with a patient's covered account
- Notice from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the practice
 - The practice is notified by a patient, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft

2. Detecting Red Flags

The practice's identity theft prevention program should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account and
- Authenticating patients, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts

3. Preventing and Mitigating Identity Theft

The practice's identity theft prevention program should provide for appropriate responses to the Red Flags the practice has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a medical practice should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a patient's account records held by the practice or a third party, or notice that a patient has provided information related to a covered account held by the practice to someone fraudulently claiming to represent the practice or to a fraudulent website.

Appropriate responses to the Red Flags may include the following:

- Monitoring a covered account for evidence of identity theft
- Contacting the patient
- Changing any passwords, security codes, or other security devices that permit access to a covered account
- Reopening a covered account with a new account number
- Not opening a new covered account
- Closing an existing covered account
- Not attempting to collect on a covered account or not selling a covered account to a debt collector
- Notifying law enforcement or
- Determining that no response is warranted under the particular circumstances

4. Updating the identity theft prevention program

Practices should update the identity theft prevention program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to patients or to the safety and soundness of the practice from identity theft, based on factors such as:

- The experiences of the practice with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft
- Changes in the types of accounts that the practice offers or maintains and
- Changes in the business arrangements of the practice, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements

5. Methods for administering the identity theft prevention program

- Oversight of program. Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:
 - Assigning specific responsibility for the identity theft prevention program's implementation
 - Reviewing reports prepared by staff regarding compliance by the practice with the Red Flags rule and
 - Approving material changes to the identity theft prevention program as necessary to address changing identity theft risks
- Reports
 - In general. Staff running the identity theft prevention program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the practice with the Red Flags rule
 - Contents of report. The report should address material matters related to the identity theft prevention program and evaluate issues such as: the effectiveness of the policies and procedures of the practice in addressing the risk of identity theft in connection with

the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the identity theft prevention program

- Oversight of service provider arrangements. Whenever a practice engages a service provider to perform an activity in connection with one or more covered accounts the practice should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, the practice could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the practice, or to take appropriate steps to prevent or mitigate identity theft.

6. Other Applicable Legal Requirements

Practices that qualify as creditors should be mindful of other related legal requirements that may be applicable, such as:

- For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation
- Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert
- Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate
- Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft and
- Though the FTC did not specifically include them in its guidance, practices are still subject to the Health Insurance Portability and Accountability Act (HIPAA), including the privacy regulations found at 45 C.F.R. Parts 160 and 164, and the full array of health care laws with which you currently comply