

Protect your patients, protect your practice: What you need to know about the Red Flags Rule

Compliance date: May 1, 2009

In November 2007, the Federal Trade Commission (FTC) issued a set of regulations, known as the “Red Flags Rule,” requiring that certain entities develop and implement written identity theft prevention and detection programs to protect consumers from identity theft. While the American Medical Association (AMA) is committed to the protection of patients and physicians, the Red Flags Rule did not specifically state whether physician practices were subject to the Red Flags requirements. In response to FTC staff indications that the FTC intends to apply the Rule to physician practices, the AMA expressed its concerns and successfully delayed implementation of the Rule until May 1, 2009. The AMA is continuing its efforts to persuade the FTC that physicians are not “creditors,” and therefore should not be subject to the Red Flags Rule. In the interim, and because of the immediacy of the May 1, 2009 implementation date, the AMA has prepared this guidance document and [sample policies for physicians](#). You can incorporate this simple identity theft prevention and detection program into your practice’s existing compliance and HIPAA security and privacy policies.

What is the purpose of the Red Flags Rule?

The Red Flags Rule requires certain entities to develop and implement policies and procedures to protect against identity theft. Identity theft occurs when someone uses another’s personal identifying information (e.g., name, Social Security number, credit card number, or insurance enrollment or coverage data) to commit fraud or other crimes. In the case of physician practices, of particular concern is medical identity theft. Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity—such as insurance information—without that person's knowledge or consent to obtain or make false claims for medical services or goods. Medical identity theft can also result in erroneous entries into existing medical records and can involve the creation of fictitious medical records in the victim’s name.

Who has to comply with the Red Flags Rule?

The Rule applies to any institution considered a “creditor.” A creditor is defined 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, however, considers physicians who accept insurance or allow payment plans to be creditors and therefore subject to the Red Flags Rule.

The FTC takes the position that physicians extend credit by allowing deferred payment until services are rendered and insurance is collected. The AMA does not believe the FTC interpretation is consistent with the intent or scope of the enabling legislation and is continuing efforts to avoid application of the Rule to physician practices. Physician practices who accept insurance or allow payment plans are covered under the Red Flags Rule and must have adequate policies and procedures in place by May 1, 2009, or they may face a penalty of up to \$2,500 per “knowing violation.”

How does the Rule differ from HIPAA privacy and security rules?

HIPAA is intended to protect personal health information (PHI) for security and privacy purposes. PHI as defined by HIPAA is covered by the Red Flags Rule, but the Rule extends to other sensitive information:

- Credit card information
- Tax identification numbers: Social Security numbers, business identification numbers and employer identification numbers
- Insurance claim information
- Background checks for employees and service providers

What is a “red flag?”

A Red Flag is a pattern, practice, or specific account activity that indicates the possibility of identity theft. The FTC identifies the following as red flags:

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious documents and/or personal identifying information, such as an inconsistent address or nonexistent Social Security number
- Unusual use of, or suspicious activity relating to, a patient account
- Notices of possible identity theft from patients, victims of identity theft or law enforcement authorities

How can my practice comply with the Red Flags Rule?

The Red Flags Rule requires that organizations have “reasonable policies and procedures in place” to identify, detect and respond to identity theft “red flags.” The definition of “reasonable” will depend on your practice’s specific circumstances or specific experience with medical identity theft as well as the degree of risk for identity theft in your practice. These policies and procedures should complement your practice’s existing HIPAA privacy and security policies and procedures that outline the administrative, technical and physical safeguards your practice employs to ensure the security of patients’ PHI.

Table 1: Procedures for addressing red flags

Element	Overview of requirements
<p>Identify what red flags could occur in your practice.</p>	<p>This procedure should outline a means to identify red flags and what occurrences may be considered a red flag, in particular¹:</p> <ul style="list-style-type: none"> <input type="checkbox"/> A complaint or question from a patient based on their receipt of another individual’s bill; a bill for a product or service that the patient denies receiving; a bill from a physician or other health care provider that the patient never patronized; or an explanation of benefits for health services never received <input type="checkbox"/> Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient <input type="checkbox"/> A complaint or question from a patient about the receipt of a collection notice from a bill collector <input type="checkbox"/> A patient or health insurer report stating that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached <input type="checkbox"/> A complaint or question from a patient about information a physician or other health care provider or a health insurer added to a credit report
<p>Indicate how you will detect red flags.</p>	<p>The procedure should identify your practice’s process to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Train staff on medical identity theft and detecting red flags <input type="checkbox"/> Assign a designated staff member to investigate possible red flags <input type="checkbox"/> Institute measures to detect red flags, such as policies on patient identity verification and authentication, address change confirmation and patient education and awareness about identity theft
<p>Establish a procedure for responding to red flags.</p>	<p>The procedure will identify the practice’s process to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Plan for gathering documentation if an incident occurs <input type="checkbox"/> Process for reporting and person to whom to report an incident <input type="checkbox"/> Guidelines for appropriate action, such as canceling the transaction, notifying the patient and/or authorities, and assessing the impact on the physician practice
<p>Review and update your practice’s red flags program at least once a year.</p>	<p>You should continually review and update your practice’s procedure and policies as applicable, based upon your practice’s experience and any changes in risk levels.</p>
<p>Incorporate specific administrative elements into your red flags program.</p>	<p>Incorporate the specified administrative elements into your red flags program:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Board of directors, appropriate committee or managing partner approve the written policy and procedures <input type="checkbox"/> A specific staff member is assigned to oversee implementation of the policy and procedures <input type="checkbox"/> All staff receive training on the policy and procedures <input type="checkbox"/> The policy and procedures are applied to arrangements with your practice’s service providers (e.g., janitorial or collection agency)

¹ World Privacy Forum, “Red Flag and Address Discrepancy Requirements: Suggestions for Healthcare Providers,” 2008.
 Copyright 2009 American Medical Association. All rights reserved.

Questions or concerns about practice management issues?

AMA members and their practice staff may e-mail the AMA Practice Management Center at [**practicemanagementcenter@ama-assn.org**](mailto:practicemanagementcenter@ama-assn.org) for assistance.

For additional information and resources, there are three easy ways to contact the AMA Practice Management Center:

- Call **(800) 262-3211** and ask for the AMA Practice Management Center.
- Fax information to **(312) 464-5541**.
- Visit [**www.ama-assn.org/go/pmc**](http://www.ama-assn.org/go/pmc) to access the AMA Practice Management Center Web site.

The Practice Management Center is a resource of the AMA Private Sector Advocacy unit.