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

New law clarifies who is subject to the Red Flags Rule

On Dec. 18, 2010, the President signed into law the "Red Flag Program Clarification Act of 2010," which clarifies the type of "creditor" that must comply with the Red Flags Rule. The American Medical Association (AMA) is pleased that this law supports AMA's long-standing argument to the Federal Trade Commission (FTC) that the Red Flags Rule should not be applied to physicians generally.

Background on the Red Flags Rule

In November 2007, the 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 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 intended to apply the Rule to physician practices and other professionals generally, the AMA, together with other professional organizations, expressed its concerns and successfully delayed implementation of the Rule five times through Dec. 31, 2010. In addition, in May 2010, the AMA Litigation Center, the American Osteopathic Association (AOA) and others filed a lawsuit in federal court seeking to block the FTC from applying the Red Flags Rule to physicians. The AMA and others also pursued federal legislation to clarify that physicians are not "creditors," and therefore should not be subject to the Red Flags Rule.

In December 2010, Congress passed and the President signed into law the "Red Flag Program Clarification Act of 2010," which limits the type of "creditor" that must comply with the Red Flags Rule. The Congressional Record further reflects the bipartisan intent of the bill's sponsors that physicians, lawyers, dentists and other professionals should no longer be classified as "creditors" for the purposes of the Red Flags Rule just because they do not receive payment in full at the time that they provide their services.

The law indicates that creditors that fall under the Red Flags Rule are only those who regularly and in the ordinary course of business: (1) obtain or use consumer reports, directly or indirectly, in connection with a credit transaction; (2) furnish information to certain consumer reporting agencies in connection with a credit transaction; or (3) advance funds to or on behalf of a person, based on the person's obligation to repay the funds or on repayment from specific property pledged by them or on their behalf (this does not include creditors who advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person). Creditors that fall under one of the above-mentioned categories must comply with the Red Flags Rule by Dec. 31, 2010. Not billing or receiving payment in full at the time a physician provides services will not

result in the physician being considered a creditor under the Red Flags Rule. The law leaves open the possibility that the FTC in future rulemaking will require other types of creditors to comply with the Red Flags Rule.

On Mar. 4, 2011, the United States Court of Appeals for the District of Columbia Circuit found the present regulations of the FTC invalid in light of the Red Flag Program Clarification Act of 2010, passed by Congress in December 2010, which shed much needed light on who is considered a creditor under the red flags rule. The Court issued the judgment in a lawsuit filed by the American Bar Association challenging the application of the Red Flags Rule to attorneys. **This Court's decision further validates the AMA's long-standing argument to the FTC that physicians who bill after rendering services are not subject to the Red Flags Rule as creditors.** In light of the Court's favorable decision and the new law, the lawsuit filed by the Litigation Center of the AMA has been dismissed.

While the AMA believes that most physicians will not fall under the categories specified under the Red Flag Program Clarification Act of 2010, the AMA has prepared this guidance document and a sample policy on identity theft prevention and detection for voluntary use.

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. Medical identity theft is of particular concern. 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 only applies to creditors who regularly and in the ordinary course of business:

1. obtain or use consumer reports, directly or indirectly, in connection with a credit transaction;
2. furnish information to certain consumer reporting agencies in connection with a credit transaction; or
3. advance funds to or on behalf of a person, based on the person's obligation to repay the funds or on repayment from specific property pledged by them or on their behalf (this does not include creditors who advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person).

Creditors that fail to comply with the Red Flags Rule could face civil monetary penalties.

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 do you 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
Identify what red flags could occur in your practice.	This procedure should outline a means to identify red flags and what occurrences may be considered a red flag, in particular[1]: ■ 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 ■ Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient ■ A complaint or question from a patient about the receipt of a collection notice from a bill collector ■ 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 ■ 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

[1] World Privacy Forum, "Red Flag and Address Discrepancy Requirements: Suggestions for Healthcare Providers," 2008.

Table 1: Procedures for addressing red flags (continued)

Element	Overview of requirements
Indicate how you will **detect** red flags.	The procedure should identify your practice's process to: ■ Train staff on medical identity theft and detecting red flags ■ Assign a designated staff member to investigate possible red flags ■ 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
Establish a procedure for **responding** to red flags.	The procedure will identify your practice's: ■ Plan for gathering documentation if an incident occurs ■ Process for reporting and person to whom to report an incident ■ Guidelines for appropriate action, such as canceling the transaction, notifying the patient and/or authorities, and assessing the impact on your practice
Review and **update** your practice's red flags program at least once a year.	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.
Incorporate specific **administrative** elements into your red flags program.	Incorporate the specified administrative elements into your red flags program: ■ Board of directors, appropriate committee or managing partner approve the written policy and procedures ■ A specific staff member is assigned to oversee implementation of the policy and procedures ■ All staff receive training on the policy and procedures ■ The policy and procedures are applied to arrangements with your practice's service providers (e.g., janitorial or collection agency)

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** for assistance.

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

- Call **(800) 621-8335** and ask for the AMA Practice Management Center.
- Fax information to **(312) 464-5541**.
- Visit **www.ama-assn.org/go/pmc** to access the AMA Practice Management Center Web site.

Physicians and their practice staff can also visit **www.ama-assn.org/go/pmalerts** to sign up for free Practice Management Alerts, which help you stay up to date on unfair payer practices, ways to counter these practices, and practice management resources and tools.

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