Red Flag Rules
By Gail Jones, AAFP

Many have already heard, but the FTC has announced that the Red Flags Rule that was to go into effect May 1st has been delayed until August 1, 2009. Originally the ruling was to begin November 1, 2008, but due to the objections of many medical associations and other organizations; the FTC had agreed to delay until May 1st. Then on May 1st, the FTC announced this new delay with the statement "to give creditors and financial institutions more time to develop and implement written identity theft prevention programs." The FTC has further agreed to provide a template to assist entities with a low risk of identity theft to comply with the law. The template is available here: http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf

But, what is the Red Flag and how does this apply to me?

The Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 require that physician offices who accept payments be compliant. These final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act were originally posted with a compliance date of November 01, 2008. Many physicians and associations have argued that practices are not creditors. **However, in a letter dated February 01, 2009, the FTC indicated that physicians may be creditors if they accept payment after the time of service.**

What is the purpose of the Red Flags Rule?

The FTC has been working for many years on ways to reduce identify theft and became increasingly aware that medical identify theft was a large problem. In an effect to protect consumers this rule was developed to eliminate medical identify theft. Medical identity theft sometimes has serious consequences caused by incorrect information included in a patient's history including diagnoses and treatments that the patient never had, wrong blood type, or incorrect allergy information, and also can lead to exhaustion of medical benefits by the imposter(s). It is often an onerous task for the patient, physicians and other providers, and health benefit plans to untangle correct patient medical and financial history from that added by an imposter. Implementation would protect not only the patients, but the providers by making it difficult for insider identify theft to occur.

Identify theft can occur in several ways. It may be as innocent as a family member or friend offering to allow someone to assume their identify and insurance when they do not have health insurance themselves. In many cases the sources of medical identify theft is from an insider who either purposefully or inadvertently releases information that is then used in fraudulent activities such as seeking care under another person's name and insurance plan or in the case of a physician's identity to order services or drugs that are

not appropriate or necessary. Without evaluating areas of risk and incorporating policies and procedures to safeguard against improper disclosures and/or provision of treatment to a person using a false identity, a practice may unwittingly become entangled in a criminal case or worse, inadvertently treat a patient based on inaccurate information. Many have questioned whether or not HIPAA addresses this issue and if the Red Flag is overkill. HIPAA does address some of the issues, but not all.

Are you subject to the Identity Theft Red Flags Rule?

It depends, if you are a cash at the time of service every time practice, than the rules do not apply to you. However, most physicians bill the patient after the claim for service has been processed by a payer and/or accept partial payments on patient balances and will then be subject to the rules. Physicians are subject to the Red Flag rule if they meet the definition of a creditor under the rule. Under the rule, a physician or practice is a creditor if they extend "credit" which means they regularly defer payment for goods or services and have covered accounts. A covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

What is considered a Red Flag?

"Red Flag" is defined as a pattern, practice, or specific activity that could indicate identity theft. For instance, if a new patient completes the date of birth on a registration form with different information than that on his driver's license, it may be appropriate to request further proof of identity. Many practices already ask for a copy of the patient's id for checks, but do not verify identification for every patient. By obtaining an id on every patient you can reduce the chances of identify theft

Some examples from the Red Flag rule that may apply to physician practices:

- 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 applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature previously obtained.

- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. 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 customers.
    - 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 persons opening accounts or other customers.
- The patient/guardian fails to provide all required personal identifying information at registration or in response to notification that the registration is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file.
- Mail sent to the patient/guarantor is returned repeatedly as undeliverable although the patient has current activity and has confirmed the accuracy of the information.
- The billing office is notified that the customer is not receiving statements and did not provide the address of record in the patient account.
- The beneficiary of a health plan contacts the practice after receiving an explanation of benefits for a service they did not receive.
- 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 (e.g., a health plan notifies the practice that claims for a patient will not be paid because the plan has determined the patient's identity was used by another party).
- An employee makes duplicate copies of forms or reports containing identifying information of patients or practice staff without known cause.
- Electronic systems security logs indicate the transfer of information to an unknown source.
- A pharmacy requests confirmation or refills of a prescription that the physician did not order.
- A request for patient information or physician authorization is received from an outside vendor for supplies or services not ordered by a physician in the practice.
- Medical records that are inconsistent with the history obtained or physician's examination findings (e.g., clear age discrepancy, surgical scarring not accounted for in surgical history)

What do I have to do then?

If you bill and accept payment, then as a creditors as defined by the rule you must:

- Develop a written program to identify, protect, and respond to possible risks of identity theft relevant to their practice and the way in which patient accounts are created and maintained in the practice.
- Periodically update the program using practice experience, changes in methods of identity theft, changes in methods of preventing identity theft, and changes in business arrangements (e.g., new outside billing or collection contracts).
- Provide oversight from owners, board of directors, or senior management including identifying a person who will be responsible for the program's implementation and review of reports and changes to the program.
- Require staff to create a report, at least annually, outlining the effectiveness of the policies and procedures 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 program.
- Take steps to ensure that service providers that conduct activities with patient accounts have reasonable policies and procedures to prevent, detect, and mitigate the risk of identity theft.

The extent of how this affects your practice will vary depending upon the size of the practice and risk factors. If you have a small practice in a long term community, it is possible that you know your patients by name, and then your risks would be considerably smaller than a large multi-speciality practice that would increase the chance of medical identify theft.

Do I need yet another manual for the practice?

Maybe, but most practices should be able to create a written Red Flag program by performing a basic risk assessment and either incorporating the activities and policies related to identifying, protecting, and responding to risks of identity theft into their existing office procedures manual, job descriptions, and HIPAA privacy and security manuals.

For instance, a small practice may create a checklist of practice policies that support the activities for preventing identity theft and then indicate for each item where the related policy already exists. This may also require development or change to some existing documents such as amending a HIPAA Business Partner Agreement to include Red Flag rule provisions.

Policy Examples:

Scheduling of Patient Appointments:
Staff scheduling an appointment will verify and document:

1. The physician or other health care professional from whom service is requested,
2. Require caller to provide patient's identifying information including patient name, date of birth, guarantor name, address, phone numbers, insurance plans and associated ID and group numbers. **Do not provide information and ask if it is correct. This is an improper disclosure of information.** (If new, advise of payment policy. If established, remind of payment policy and especially importance of bringing most current insurance ID card.)
3. Patient's current account status (if outstanding balance, request payment or transfer to billing dept.)
4. The reasons or conditions for which services being requested (e.g., routine physical and back pain)
5. Patient's language preference and/or any accommodations needed for service
6. Request that new patients authorize release of past medical records prior to first visit. Request that established patients report recent encounters with other physicians or providers and notify clinical staff of possible need to obtain records.

All new patients/guarantors are to be instructed to bring a government issued photo identification card and present this along with their health insurance card at check-in.

Shielding against problems

While considering how to detect red flags of ID theft from outside the practice, think about the internal risks of identity theft for physicians and staff within your practice. Though it may not be pleasant to contemplate, many physicians and practices have found themselves victim to misuse or theft of information by an employee or associate who had access to personally identifying information. While such instances cannot always be prevented, development and enforcement of policies and procedures for handling of such information shows the practice's commitment to safeguarding information and deterring careless or wrongful acts.

Summary

While it appears that medical practices have additional time to become compliant, it is doubtful that this is going away. In many ways, by following the Red Flag Rules the practice will not only be protecting the patients, but themselves against medical identify theft.

Red Flag Rules resources

http://www.aafp.org/online/en/home/practicemgt/regulatory-compliance/id-theft.html
http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm
http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.shtm

http://www.mgma.com/redflagsrule
http://www.aha.org/aha/advocacy/compliance/redflags.html