

Red Flags Rule: Do the Red Flag Rules apply to my medical practice?

As you are already aware, the Red Flag Rules and Guidelines went into effect January 1, 2008, with a compliance deadline that was postponed until May 1, 2009. In an effort to help members become familiar with what is required by the Red Flag Rules and how to prepare the written Program that is federally mandated and subject to enforcement under the Fair Credit Reporting Act (FCRA) by the Federal Trade Commission (FTC), your newsletters will address a different compliance issue, each week, over the next few months.

The definition of both a "creditor" and an "account covered" are key in determining whether or not you are subject to the Red Flag Rules. A *creditor* is defined as any entity that regularly extends, renews or continues credit. Credit includes, in part, transactions in which you defer payment of debts or accept deferred payment for products or services. One primary example is that of a patient who makes payment after the date of service; this type of arrangement constitutes an extension of credit. If you accept insurance and the patient is ultimately responsible for any balance after insurance payment is received, this is an acceptance of deferred payment and you are a creditor. However, accepting credit cards as a form of payment for products or services rendered at the time of the product purchase or service rendered does not by itself result in your being classified as a creditor under these new rules.

If you determine that you are a creditor, as defined under the Red Flag Rules, the next step is to determine whether your practice has "covered accounts." A *covered account* is defined as any account that a creditor offers or maintains used primarily for personal, family, household purposes that involves or permits multiple payments or transactions. However, a covered account also includes any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers from identity theft.

In the great majority of medical practices, the Red Flag Rules will apply because accepting insurance generally results in deferring payment from a patient until payment is received from the insurance carrier. This determination is important because the Red Flag Rules require creditors with accounts that are covered to identify those accounts that are at risk, and to define, detect, and respond to the red flags in order to prevent or at least mitigate identity theft. In short, a primary goal of a physician is to recognize suspicious circumstances that would prompt your office to be alert for possible theft of a patient's identity and to respond accordingly.

Red Flag Rules Tip: Establishing an Identity Theft Prevention Program

If you are a creditor as defined under the Red Flag Rules, and your medical practice opens and maintains covered accounts, then you are required to prepare and implement a written Identity Theft Prevention Program.

The written program should serve to accomplish specific goals:

- Identify theft that may or does occur in connection with either the opening or the maintaining of the covered account. The Rules further require that you identify relevant red flags for covered accounts. Relevant to your medical practice might include the types of accounts offered and maintained, the method(s) used to open accounts (including who has access when opening covered accounts and in maintaining covered accounts), who collects on these accounts and the identifying information relating to a patient. Also relevant would be any prior exposure or experience your medical practice has had regarding identity theft.
- Detect red flags that are incorporated into your written program.
- Respond appropriately to red flags that are detected. This would include review of your written program to ensure detection of red flags that have been identified for inclusion, and then (re)acting to prevent or mitigate identity theft.
- Periodically reviewing and updating the written program to ensure its relevance to the types of accounts and the information.

With regard to requirements under the Red Flag Rules, the FTC has issued Red Flag Guidelines that are to be considered when preparing your written program. The guidelines include specific examples of the requirements. At this time, MedChi is providing an overview of each requirement, and will subsequently address the specifics on how to move forward with the guidelines for compliance.

Red Flag Rules: Administration of an Identity Theft Prevention Program

Last week's TIP addressed establishing an Identity Theft Prevention Program and included key considerations to be incorporated. In sum, a written program that is developed and implemented needs to function to detect, prevent, and mitigate identity theft in connection with covered accounts. The size and complexity of your written program will depend on the medical practice or office setting, as well as the nature and scope of your medical practice. More specifically, your office needs to develop and implement reasonable policies and procedures to identify relevant Red Flags in connection with the opening and maintaining of covered accounts.

Once you have identified the necessary elements to include in your written program ([see TIP #2](#)), the next step is the administration of the program. Pursuant to the FTC Red Flag Rules, 16 CFR Part 681.2(e), there must be continued administration of the program. Continued administration includes someone of senior level administration who is designated as responsible for oversight, development, implementation and administration of the program. Staff is to be trained as necessary in order to effectively implement, continue and ensure ongoing success with the program. In short, someone within your office who is responsible for exercising appropriate and effective oversight must be designated. The rules also require that in the absence of a board of directors or other appropriate committee, that initial approval of the written program by senior level administration be obtained.

In addition to the rules, there are specific guidelines that the FTC requires be considered. The specific guidelines relating to these rules will be addressed in a subsequent

newsletter. Remember, that the guidelines outlined in these rules must be considered, but need only be incorporated into your written program as appropriate.

Red Flag Rules: Sources That Must be Considered

Included in the FTC Red Flag Rules and Regulations are guidelines that must be considered when developing and providing for the continued administration of your written program. Required consideration of the guidelines includes reviewing the procedures appropriate to detect, prevent and mitigate identity theft in connection with covered accounts. The goal of the guidelines is to assist in your formulation and maintenance of the written program.

Important to note is that a practice may incorporate, as appropriate, existing policies, procedures and other arrangements that "control reasonably foreseeable risks" to patients or to the safety and soundness of the creditor from identity theft. In addition to those risk factors of which you may already be aware, the guidelines require that you consider the following specific risk factors to determine whether there is a reasonably foreseeable risk to your patients (risk to the safety and soundness of their identifying information) of identify theft:

- the type of accounts offered and/or maintained
- the methods used to open a covered account
- the methods used to access covered accounts, and
- previous experience your office has had with identity theft

Each of these factors should be reviewed to determine its relevance to your medical practice. One example of a red flag that may occur in your practice setting would be where a driver's license picture and name do not exactly match the name on the insurance card. Another example would be the name on a credit card provided for balance owed not matching the patient information you have on file.

Included in the FTC guidelines is consideration of sources of possible identity theft. Sources include knowledge of prior incidences of patient identity theft or attempted theft of personal and/or identifying information, as well as possible methods of identity theft that may occur within your practice setting. In addition, the guidelines provide that supervisory guidance should be considered where applicable. This would include guidance or information you have discovered from MedChi or other organizations, as well as regulatory agencies, regarding identified sources of possible identity theft.

Red Flag Rules Tip: Detection of Red Flags and Examples

As outlined in an earlier newsletter, your written program, designed and implemented to prevent identity theft, is intended to detect red flags related to identity theft. The potential of identity theft is most likely when registering a new patient, where your office is also opening a new account. However, it is required that your written program be operational on an ongoing basis to ensure a continuous effort is made in preventing, as

well as mitigating, identity theft. One example of an office policy and procedure regarding ongoing efforts would be to check for any changes in patient information during return visits. An example might be the procedure followed in the event of suspicious personal identifying information presented during an office visit. One case in point involved a patient who did not have health insurance who presented his brother's license and insurance information. Based on their limited age difference, as well as the relative infrequency of licensure pictures, this case of identity theft went undetected until the brother whose identity had been stolen received a bill for the balance owed for medical services.

In preparing your policies, remember to include information about identity theft that you may have learned or discovered from other sources such as colleagues, regulatory agencies and other organizations ([see Tip # 4](#)). The case described above is an example of identity theft that, if relevant to your practice, should be considered when preparing your program. It is quite likely that many of the requirements of the written program are policies and procedures already in place in your medical practice. Your preparation of a list of current office policies and procedures regarding the management of identifying information, patient documents, and monitoring transactions, would provide a baseline to then begin a review of what is specifically required by the Red Flag Rules and Guidelines.

Red Flags Rules Tip: Preventing and Mitigating Patient Identity Theft

Under the Red Flag Guidelines, it is required that you consider certain responses relating to the prevention and mitigation of identity theft. In the event that you detect possible identity theft, appropriate responses to the red flag(s) should be proportionate and adequate when considering the degree of risk posed. An appropriate response to detection would include an assessment of related factors that may increase the identity theft risk. One example might be in the case of a breach of patient identifying information that results in unauthorized access to a patient's account records. A second example might involve someone who has fraudulently claimed that he is one of your patients. How you would respond to these types of red flags should be included in your written program. Guidelines regarding possible responses include the following:

- Monitor covered accounts for evidence of patient identity theft;
- Communicate with your patient upon detection of possible identity theft;
- Change security information such as passwords or other codes in response to a red flag indicating possible identity theft;
- Close out accounts as necessary and where appropriate re-open with different identifying and secure information;
- Not pursuing a patient for debt owed where there is reasonable evidence of identity theft;
- Notifying the proper authorities;
- Determine that in a particular case no response is necessary based on the circumstances.

Important to remember is that these guidelines should be considered when preparing your program, and that appropriate and reasonable responses that are relevant to your medical practice should necessarily be included in your policies and procedures.

Red Flag Rules TIP: Administering the Program

Included in the FTC Red Flag Guidelines are methods for administering the required written program. In short, you are required to have oversight by senior level management within your practice, reports relating to the administration of the program and oversight of service provider arrangements your office regarding patient accounts.

More specifically with respect to each of these three administration aspects is the following:

- *Oversight within your practice*, by designated senior level management, includes the responsibility for implementing the written program, reviewing documents and reports prepared by other staff and relating to compliance with identity theft prevention, detection and mitigation and approving changes as necessary to address changing risks of identity theft.
- *Reports* includes evaluation of issues such as the effectiveness of your office policies and procedures, changes to your program based on information you have discovered or received and recommendations for changes. Responsibility for reporting includes the development, implementation and administration of the program, as well as periodic evaluation and updating. The guidelines provide for annual reporting, by senior staff level management, regarding compliance with the program. Based on the size of your practice, reporting may be as limited as office manager reporting to a solo practitioner. However, in large practice settings, reporting by senior level management may well be to a board of directors.
- *Oversight of service provider arrangements* includes steps to ensure that reasonable policies and procedures are in place to detect, prevent and mitigate the risk of identity theft when patients' personal and identifying account information is shared. One example would be where your office outsources billing. Please keep in mind that the May 1, 2009 deadline for compliance with these new FTC Rules is approaching quickly, and that MedChi is here to support you in your efforts to comply with this mandated written program.

Information compiled and distributed by MedChi, The Maryland State Medical Society, 2009.