

Red Flag Rules: What You Should Know

In November 2007, The Federal Trade Commission (FTC) issued regulations that aimed to protect consumers from identity theft. The regulations required financial institutions and creditors with covered accounts to implement a written identity theft prevention program. The program must provide for the identification, detection, and response to patterns, practices, or specific activities (known as ‘red flags’). Under the FTC’s guidelines, physicians who regularly bill their patients for services rendered (including copayments and coinsurance) are considered creditors and must comply with the regulations. **The compliance date for the prevention program is November 1, 2009.**

Chiropractic practices that defer payments must create and execute an identity theft protection plan in order to meet the requirements of the Red Flag Rule.

<u>FTC Policy</u>	<u>Recommended Procedure</u>
<ul style="list-style-type: none"> Identify relevant red flags (patterns, practices, and specific forms of activity that signal possible identity theft) and incorporate them into your program 	<p>Warning signs include –</p> <ul style="list-style-type: none"> Alerts, notifications, or warnings from a consumer reporting agency; Suspicious documents; Suspicious personally identifying information; Suspicious activity relating to a covered account; or Notices from customers, victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts.
<ul style="list-style-type: none"> Detect red flags 	<ul style="list-style-type: none"> Obtain identifying information about the person opening a covered account then verify their identity.
<ul style="list-style-type: none"> Prevent and mitigate identity theft 	<ul style="list-style-type: none"> Authenticate clientele, monitor transactions, and verify the validity of change of address requests in the case of existing covered accounts. Monitor a covered account for any indication of identity theft (red flags). Contact the client. Change any secret codes (passwords, security codes, security devices, etc) that permit access to a covered account. Reopen a covered account with a

- Update your program periodically
- different account number.
- Do not open a new covered account.
- Always close an existing covered account.
- Do not attempt to collect on a covered account or sell a covered account to a debt collector.
- Notify law enforcement when needed.
- Determine that no response is warranted under the particular circumstances.
- The program requires changes in methods of identity theft in order to detect, prevent, and alleviate identity theft.

How does a Doctor of Chiropractic Comply with the Red Flag Rules?

When identifying red flags, consider the nature of your business and the type of identity theft to which you might be vulnerable. Because health care providers may be at risk for medical identity theft, you'll need to identify the warning signs that reflect this risk. Consider the following table which gives guidelines on developing the FTC regulated protocol:

Step 1 Appoint a staff member to develop the compliance plan. Make certain the "compliance regulator" is able to set aside a considerable amount of time in order to develop and implement the plan.

Step 2 The compliance regulator should first determine if the chiropractic practice meets the definition of a 'creditor' who works with covered accounts (any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit).

Step 3 If the chiropractic practice falls under FTC's definition of 'creditor', the compliance regulator should perform an analysis and risk assessment of the practice's current policies and procedures for fraud transactions. Once the compliance regulator has determined what transactions increase the risk of identity theft, he/she should develop policies and procedures to alleviate the possibility of theft. Each transaction should include a policy explaining how the practice will identify, detect, and respond to red flags.

Examples of policies are as follows:

Identify new patients by checking a photo ID.

Match the patient's insurance information to their ID.

Contact law enforcement immediately if you receive notice that a patient or consumer has been the victim of identity theft.

Determine how past issues were dealt with when identity theft had occurred.

ACA recommends compliance regulators consult with their internal HIPAA policies and procedures manual as there could be potential overlap with your identity theft compliance plan. FTC's rule allows for flexibility in tailoring the compliance program. If it is determined your chiropractic office has a low risk of identity theft then developing a program should be simple and straightforward, with only a few red flags needed.

Step 4 Follow the appropriate steps in order to approve the compliance plan; consult with your board of directors, committees, owners, when suggested.

Step 5 Staff who are in regular contact with clients should be trained on the red flag compliance plan. A staff meeting with training material is recommended. ACA believes the key step to enforcing this plan is adequate training. Remember, FTC may seek civil penalties of \$2500 per violation.

Step 6 The compliance regulator should re-evaluate the plan annually to determine if modifications need to be made. If changes are required, staff should be re-trained on those specific changes.

For additional information, please access these resources:

Guidelines: <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf> (The Guidelines are on pages 63773-63774 of the document.)

Federal Register Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, <http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf>

The "Red Flags" Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft, <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>

Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf