Red Flag Rules Apply to Doctors of Chiropractic

Compliance date: May 1, 2009

BACKGROUND: Based on legislation passed by Congress in 2003, in 2007, the Federal Trade Commission (FTC) first issued regulations stating that financial institutions and creditors are required to develop and execute written "identity theft prevention programs" that must provide for the identification, detection, and response to patterns, practices, or specific activities. These are known as "red flags" and could indicate identity theft. Enforcement of the regulation begins May 1, 2009.

Until recently, there was much ambiguity regarding the regulations and questions were raised as to whether physician offices fell under the FTC red flags guidelines. In February, the FTC issued a statement clarifying that Identity Theft Red Flag Rules do indeed apply to physicians including doctors of chiropractic. The FTC does not believe that the regulations will inflict any substantial burdens on most healthcare providers despite the fact that several specialty groups have objected to the inclusion.

ACA ACTION: The American Chiropractic Association (ACA) is supporting congressional intervention in this issue and is behind a letter to be sent to the FTC by the Chairwoman of the House of Representatives Committee on Small Business, Rep. Nydia Velázquez (D-NY) urging FTC to hold the enforcement of the Red Flags Rules in abeyance, until further effects of the rules are examined. **However, please treat the regulations as "live" until further notified by the ACA.**

WHY NOW? The goal of the Rules is "to reduce the overall incidence and impact of identity theft, including medical identity theft" along with credit information. Medical identity theft occurs when someone uses another person's name and sometimes other parts of their identity, such as insurance information, without the person's knowledge or consent.

Two conditions must be met in order for medical practices to be covered; they need to be a **"creditor"** organization, and they are required to have **"covered accounts."** "Credit" is defined as an arrangement by which you defer payment of debts or accept deferred payments for the purchase of property or services. If a medical practice first submits a claim for services to an insurance company and then bills any remaining amount to the patient after the claim is adjudicated, it is considered a "creditor" organization in addition to a creditor arrangement since payment for goods and services is deferred until the claim is processed. Red Flag Rules consider patient billing records "covered accounts" if they permit multiple payments or if they have a reasonable risk of identity theft. Red Flag Rules are risk-based and designed to be flexible based on the level of risk faced by each health care provider.

WHAT YOU NEED TO DO: Again Red Flag compliance plans must be in place by **May 1, 2009**. So, what should you to do protect yourself? The FTC suggests that you consider **implementing a program that best suits your practice as long as it meets certain basic requirements.**

The FTC states that : "…for most physicians in a low risk environment, **an appropriate program might consist of checking a photo identification at the time services are sought and having appropriate procedures in place in the event the office is notified – say by a consumer or law enforcement – that the consumer's identity has been misused."**

The information below is supplied by the FTC. Specifically, the FTC suggests that there are four basic steps to designing a program to comply with the regulation:

1. Identify relevant red flags;
2. Detect red flags;

3. Prevent and mitigate identity theft; and
4. Update your program periodically.

In addition, your program must spell out how it will be administered. The program should be appropriate to the size and complexity of your company or organization, as well as the nature of your operations.

According to the FTC, physician offices with covered accounts (see above) must develop a written program to identify the warning signs of identity theft.

Below are the categories of warning signs — red flags — that your program must identify and address:

- 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.

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.

Questions? Please Access These Additional Resources:

FTC Guidelines: http://www.acatoday.org/pdf/57_58.pdf

Full Federal Register Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (issued 2007), 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