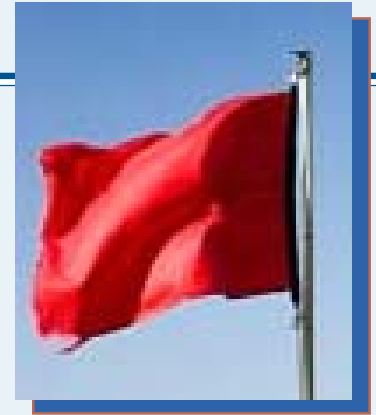


FTC Sends Red Flag Signal to Medical Practices

By Jon Waitukaitis, Audit Supervisor, Anders Minkler & Diehl LLP

While you may not think identify theft is a major problem for medical practices, the Federal Trade Commission (FTC) has a different opinion, and they have put measures in place to stop it. In fact, the time for medical practices to comply with the Red Flag Identity Theft Rules is May 1, 2009!

Designed to detect, prevent, and mitigate identity theft in connection with “covered” accounts, this new rule was issued by the FTC under the Fair and Accurate Credit Transactions Act (FACTA). It requires financial institutions and other “creditors” to develop and implement a written identity theft prevention program.



Why Health Care Providers?

Since this is essentially required of financial institutions, many health care practices are asking “why me?” Here’s why: if a health care provider extends credit to a consumer by establishing an account permitting multiple payments, the provider is a creditor offering a covered account and is subject to the Red Flag Identity Theft rules. This ruling applies to dental practices and hospitals as well as any other health care provider that allows a patient to receive services but pay at a later date.

A “creditor” is considered “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or contribution of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.”

Under this scenario, medical practices that allow patients to pay over time are “creditors” and subject to compliance under FACTA. The term creditor also applies to any third party attempting to collect payment on behalf of a hospital.

Under this new ruling, the term “covered” account is defined very broadly. Red Flag Rules apply to:

- An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, and
- Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. **Medical practices fall into this category as it includes patient billing records.**

Other Instances of Identity Theft

Health care providers also confront a unique issue that is not faced by other creditors: how to deal with potential medical identity theft. Medical identity theft is a subset of identity theft, and occurs when erroneous entries are put into medical records, or false records created, due to identity theft.



Jon Waitukaitis, a member of the AMD Health Care Services Group, is also a member of the firm’s Fraud Prevention Group. Questions and comments can be addressed to Jon at jwaitukaitis@amdcpa.com.

What Does It Take To Comply?

In order to be in compliance with the Red Flag Identity Theft Rules, practices must develop a written identity theft prevention program that includes policies and procedures for detecting, preventing and mitigating identity theft in connection with new or existing accounts. Specifically, the program must:

- 1) Identify patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft, and incorporate those red flags into their program
- 2) Detect red flags that have been incorporated into the program
- 3) Respond appropriately to any red flags that are detected
- 4) Make sure the program is updated periodically to reflect changes in risks from identity theft.

Administration of the program requires the practice to:

- 1) Secure approval of the initial Program from the board of directors (or board committee)
- 2) Designate a senior management member to oversee and administer the Program, including review of staff compliance reports
- 3) Train staff as necessary to implement the Program effectively
- 4) Ensure, when it engages a service provider to perform an activity on its behalf (such as one that opens accounts), that the activity is conducted in compliance with a Program that satisfies the rules.

In addition to requiring adoption of an Identity Theft Prevention Program, FACTA contains provisions applicable to users of consumer reports and to credit card issuers. If you request consumer reports, or if you issue “smart cards” to patients to be used at the point of service, these provisions will apply to you as well.

Non-Compliance Could Cost You

Non-compliance penalties include fines of \$3,500 (increased from \$2,500 effective February 9, 2009) per covered account and the risk of civil liability. For repeated violations after an order to comply, the FTC could file suit seeking several times that for each violation.

For now, it would be prudent to incorporate a simple identity theft prevention and detection program into existing compliance and HIPAA security and privacy policies.