HARRISBIOMEDICAL™

COMPLIANCE SERVICES

FACTA AND THE RED FLAGS RULE

The Fair and Accurate Credit Transactions Act of 2003 included a provision known as the "Red Flags" Rule, which took effect in January 1, 2008, although the compliance deadline was extended to August 1, 2009. The rule requires many businesses and organizations to implement written Identity Theft Prevention Programs designed to detect the warning signs or "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts. By identifying red flags in advance, you will be better equipped to spot suspicious patterns when they arise and take steps to prevent a red flag from escalating into identity theft. The Red Flags Rule is enforced by the Federal Trade Commission (FTC).

ARE MEDICAL & DENTAL OFFICES SUBJECT TO THE RED FLAGS RULE?

There have been challenges to FTC's position that health care businesses, including dental offices are subject to the rule if they extend credit. The Red Flags Rule applies to "financial institutions" and "creditors." The determination of whether a business is subject to the Red Flags Rule isn't based on the industry, but on whether the business' activities fall within the relevant definitions:

> **Creditor:** A "creditor" includes businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later. The rule also defines a "creditor" as one who regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions including anyone who regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit.
>
> **Covered Accounts:** A "covered account" is a consumer account you offer your patients for personal or family purposes that permits multiple payments or transactions. An additional definition of "covered account" is "any other account that a 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, including financial, operational, compliance, reputation, or litigation risks."

DON'T OUR HIPAA PROGRAMS PROTECT AGAINST IDENTITY THEFT?

Your existing HIPAA Privacy and Security programs play an essential role in keeping patients' personal information from falling into the wrong hands or being used improperly. But your HIPAA programs won't prevent a resourceful thief from becoming your patient using a stolen or false identity and running up a bill you'll never be able to collect. The Red Flags Rule picks up where HIPAA leaves off. It seeks to prevent identity theft by ensuring that your practice is on the lookout for the signs that a patient or prospective patient is using someone else's information to get services from you with no intention of paying.

If you've concluded that your dental practice is a creditor, you must determine if you have any "covered accounts," as the Red Flags Rule defines that term. You need to implement a written program only if you have covered accounts. The Rule requires you to conduct a periodic risk assessment to determine if you have "covered accounts."

If you're a creditor or financial institution with covered accounts, you must develop and implement a written Identity Theft Prevention Program. The Program must be designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones. Your Program must be appropriate to the size and complexity of your business or organization and the nature and scope of its activities.

YOUR IDENTITY THEFT PREVENTION PROGRAM

The Red Flags Rule sets out how, if you are subject to the rule, you must develop, implement, and administer your Identity Theft Prevention Program. Your Program must include four basic elements, which together create a framework to address the threat of identity theft:

- Your program must include reasonable policies and procedures to identify the "red flags" of identity theft you may encounter in the day-to-day operation of your dental practice. Red flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. For example, if a patient has to provide some form of identification to open an account with your practice, an ID that looks like it might have been altered would be a "red flag".
- Your program must be designed to detect the red flags you've identified. For example, if you've identified suspicious IDs as a red flag, you must have procedures in place to detect possible phony, forged, or altered identification.
- Your program must spell out appropriate actions you'll take when you detect red flags.
- Your program must address how it will be re-evaluated periodically to reflect new risks, because identity theft is an ever-changing crime.

The Red Flags Rule sets out requirements on how to incorporate your program into the daily operations of your practice. The business owner (doctor) must approve your first written program (the board of directors must approve the program in corporate practices). Your program must state who is responsible for implementing and administering it effectively. Because your employees have a role to play in preventing and detecting identity theft, your program also must include appropriate staff training. If you outsource parts of your operations that would be covered by the rule (such as patient billing) your program also must address how you will monitor your contractor's compliance.

The Red Flags Rule gives you the flexibility to design a Program appropriate for your practice based on its size and potential risks of identity theft. While some dental practices may need a comprehensive program that addresses a high risk of identity theft, others with a low risk of identity theft could have a more streamlined program.

FOUR STEPS TO COMPLIANCE WITH THE RED FLAGS RULE

1. **Identify relevant red flags.** Identify the red flags of identity theft you're likely to encounter in your dental practice.
2. **Detect red flags.** Set up procedures to detect those red flags in your day-to-day operations.
3. **Prevent and mitigate identity theft.** If you spot the red flags you've identified, respond appropriately to prevent and mitigate the harm done.
4. **Prepare/update your Program.** The risks of identity theft can change rapidly, so it's important to keep your program current and educate your staff.

DO YOU HAVE TIME TO COMPLY WITH THE RED FLAGS RULE?

We do. Harris Biomedical can answer any questions you have about FACTA and the Red Flags Rule and help you with compliance: from conducting your Identity Theft Risk Assessment to preparing your written program, and training your staff. Call 866-548-2468 or e-mail info@harrisbiomedical.net.