



**060410 BLAST**

## **RED FLAGS RULE DELAYED UNTIL DECEMBER 31, 2010**

After several threats to be effective June 1, 2010, the Federal Trade Commission's (FTC) Red Flags Rule implementation has again been delayed until December 31, 2010.

The Red Flags Rule requires creditors and financial institutions to develop identity theft prevention programs. The FTC considers healthcare providers to be creditors in cases where they accept the patient's insurance and bill the patient after the insurance has paid, or in cases where patients setup payment plans with the practice; these are deemed to be 'covered accounts', i.e., subject to the Red Flags Rule.

If a practice determines that it qualifies as a creditor that maintains 'covered accounts', the Red Flags Rule requires the practice to develop an identity theft prevention program that contains "reasonable policies and procedures" (and can incorporate existing procedures) to achieve the following goals:

1. Identify relevant indicators of a possible risk of identity theft ("Red Flags"), i.e., past identity theft incidents at the practice, types of accounts offered.
2. Detect Red Flags – The practice should always validate the identity of the patient when opening new accounts and validate address changes for existing accounts.
3. Preventing and Mitigating Identity Theft – The practice's identity theft prevention program should provide for appropriate responses to the Red Flags the practice identifies according to the risk posed, i.e., changing security codes and passwords in cases where data security is breached.
4. Updating the identity theft prevention program – Practices should review and update their identity theft prevention program regularly to reflect changes in risks to patients or security breaches.

More information and suggestions for developing an identity theft prevention program can be found on the FTC Red Flags Rule webpage at:

<http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>