



## **Health IT and Federal Trade Commission's-Red Flag Rules**

Medical practices and health providers are prime targets for security breaches of personal information (address, date of birth, social security number, etc., of a patient), financial information (patient's bank account numbers, credit card numbers, etc.) and medical records (medications, HIV status, mental health or addiction issues, etc.). The move to Health IT (electronic communication and filing systems) escalates the risk that sensitive information could be subject to theft or misuse. In response to Identity Theft, the Federal Trade Commission (FTC) has initiated "Red Flag Rules" and "Identity Theft Prevention Program" that are meant to prevent or limit damages caused by theft of personal information.

The FTC requires financial institutions and other creditors to create written identity theft prevention programs designed to prevent, detect, and mitigate the effects of identity theft. These regulations are applicable to creditors including health care providers that offer financing or payment plans. The written identity theft program must contain policies that identify "red flags," including relevant patterns, practices and/or activities that potentially implicate identity theft, detect the "red flags" that are identified in the program, respond to "red flag" incidents that are detected in order to prevent and mitigate the effects of identity theft; and ensure that the program is reviewed and updated periodically in order to adjust to changing and developing identity theft risks.

The incidents or activities that constitute "red flags" of identity theft will vary based upon the size of the medical practice or business. Medical entities may find that their red flags will fall under some or all of the following categories: 1) alerts received from a consumer credit reporting agency; 2) suspicious documentation that appears to be altered or inconsistent with other documents on file; 3) suspicious personal identifying information, such as multiple addresses; 4) unusual or suspicious use of or access to a patient's covered account; or 5) notification from patients or law enforcement authorities indicating suspected or actual identity theft.

The FTC has the authority to impose a penalty of \$3,500 per incident of a knowing violation of the Rules. At the request of "Members of Congress", the Federal Trade Commission has delayed enforcement of the "Red Flags" Rule until June 1, 2010.