

## FTC Red Flag Laws and Health Care Providers

Stephen G. Prom, Esq. and Kristen A. Foltz, Esq.  
Health Law Attorneys with Akerman Senterfitt

Most people think of “identity theft” in relation to a stolen credit card or a hacked computer. Not many people would worry about such theft after a trip to the doctor or hospital. Then again, how many times does a person’s social security number, date of birth, and other personal information appear in medical records?

### What is Identity Theft?

Federal law defines “identity theft” as “a fraud committed or attempted using the identifying information of another person without authority.” [16 C.F.R 603.2(a)].

The Federal Trade Commission (FTC), defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—(1) name, social security number, date of birth, official State or government issued driver’s license...18 U.S.C. 1029(e)

### What are the Red Flag Rules?

In 2003 President Bush signed the Fair and Accurate Credit Transaction Act (FACTA). The goal of FACTA was to protect consumers against identity theft by requiring regulators to make a list of “Red Flags” that signify identity theft. From this sprang the FTC’s Identity Theft Red Flag Rules.

The American Medical Association (AMA) recently wrote a letter to the FTC asking for clarification of the rules. It requested, “that the FTC withhold any plans to apply the Red Flag Rules to physicians until this matter is resolved.”

The rules were supposed to be effective November 2008, however, the FTC recently decided to suspend enforcement of the rules until May 1, 2009 in order to give providers more time to develop their identity theft prevention programs.

Health care providers that meet the FTC’s definition of “creditor” and whose clients have “covered accounts,” have to introduce a program that identifies, protects against, and alleviates identity theft.

The term “creditor” includes “a person who arranges for the extension, renewal, or continuation of credit, which in some cases could include third-party debt collectors.” [15 U.S.C. 1961a(e).]

The FTC defines “covered account” as: (i) 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, such as a credit card account... (ii) 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....41.90(3).

Thus, depending on the type of account, health care providers could meet the definition and have to enact identity theft protections.

### What are the FTC Red Flag Rules?

The program is flexible, allowing health care providers to design their own system to meet their needs in fighting identity theft. In fact, the FTC states that “the Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.” 41.90(d)(1).

One requirement is having the institution’s Board of Directors approve and be involved in the oversight, development, implementation and administration of the program. Also, staff training is a key component to the program.

A corollary to the Red Flag Rules is Florida’s Breach Notification Law. While it addresses what to do after an information breach occurs, it serves as additional motivation due to administrative fines for those health care providers resisting implementing an identity theft policy.

The Breach Law, Florida Statute Section 817.5681(1)(a), requires “any person who conducts business in this state and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system.”

As it applies to health care providers, patients must be notified when a breach of unencrypted electronic information occurs.

### Identity Theft Prevention Tips

1. Have policies and procedures for background checks, account/password security, information access, use monitoring, and reporting
2. Decrease the use of social security numbers, birthdates, and other identifiable personal information
3. Assign specific User Codes and upon issuance, have the employee sign an agreement reiterating the confidentiality/privacy obligations, limited access, and log off procedures
4. Design computer prompts reminding to keep protected information safe
5. Keep computer virus and spam software updated

For more information, go the Akerman Senterfitt law firm’s web site at [www.akerman.com](http://www.akerman.com).