PLUNKETT COONEY

Will Healthcare Providers Soon Wave FTC's Red Flags?

October 14, 2008

The Federal Trade Commission (FTC) has recently issued regulations that likely require healthcare providers to implement identity theft programs. These regulations are commonly referred to as the "Red Flag Rules."

The Fact Act (FACTA) was signed into law on Dec. 4, 2003. FACTA amended the Fair Credit Reporting Act of 1970 (FCRA) to require six federal agencies to issue joint regulations and guidelines regarding the detection, prevention and mitigation of identity theft. The joint final rules and guidelines became effective Jan. 1, 2008. The mandatory compliance date for these rules is Nov. 1, 2008.

In general, the rules require covered financial institutions or creditors to develop and implement a written identity theft prevention program to detect, prevent and mitigate identity theft in connection with future and certain existing accounts.

For healthcare providers and similar entities, the likely regulatory coverage arises from the FTC regulations codified as 16 CFR Part 281, et seq.

Recently, an FTC representative made a non-binding statement that in all likelihood, most healthcare providers and similar entities will be bound by the Red Flag Rules. The FTC's current thinking (subject to change) is that the Red Flag Rules apply to an individual healthcare entity:

1. If the entity uses consumer reports for making employment decisions regarding employees or for making credit decisions with respect to patients, and/or;
2. If the healthcare entity qualifies as a "creditor" and maintains covered accounts.

Following is a list of terms applicable to the Red Flag Rules:

Creditor is defined as an entity regularly extending, renewing or continuing credit or regularly arranging for the extension of credit.

Credit is defined as the right granted by a creditor to a debtor to defer payments for goods or services. Per an FTC representative, speaking unofficially, it is likely that healthcare providers extend credit to patients when they do not demand payment for medical goods or services at the time the goods or services are provided.

© 2026 Plunkett Cooney, PC

Account is defined as a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purpose.

Covered accounts are one or both of the following:

- Accounts that the entity maintains primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions
- Accounts that the entity offers or maintains for which there is a reasonably foreseeable risk to customers from identity theft

As stated above, it appears that the FTC will find most healthcare providers to be subject to the Red Flag Rules. There are certain basic program requirements which will apply to all covered institutions including healthcare entities. Some of these program requirements include: (1) a written plan; (2) a mechanism to identify "red flags" (i.e. relevant patterns, practices and other activities which signal possible identity theft); (3) a method of "red flag" detection; (4) a method of response to detected "red flags" to prevent and/or mitigate identity theft or ensuing harm; and, (5) a process to ensure program remains updated periodically to account for potential changes in risk.

The extent and complexity of the requirements will be dependent upon the risk factors, size, nature and scope of each entity's activities. A healthcare entity's HIPAA privacy and security compliance program may provide some coverage, or at the very least, the foundation upon which to build and create a red flag compliant program.

© 2026 Plunkett Cooney, PC