

Health Care Providers and Identity Theft – Ensuring Compliance with the “Red Flags” Rule

Lora M. Jennings
Martin, Pringle, Oliver, Wallace & Bauer LLP

Beginning August 1, 2009, the Federal Trade Commission will start enforcing the Red Flags Rule – a law that requires certain businesses and organizations, including healthcare providers, to develop and implement a written program to identify, detect, and respond to warning signs, or “red flags,” of identify theft.¹ A “red flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft.”

Whether a particular healthcare provider is required to comply with the Red Flags Rule depends on whether the provider’s activities qualify the provider as a “creditor” who maintains “covered accounts.” The Red Flags Rule defines a “creditor” to include any entity that regularly defers payments for goods or services and bills the customer after services are rendered. “Covered accounts” are defined to include those accounts that the creditor offers or maintains “primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions” and any other account “for which there is a reasonably foreseeable risk to customers” or to the creditor from identify theft.” If a healthcare provider requires full payment at the time the services are rendered, or accepts only direct payment from Medicaid or a similar program, the Red Flags Rule would not apply. At the same time, however, healthcare providers must periodically reassess whether it offers or maintains any “covered accounts.”

A healthcare provider that qualifies as a “creditor” with “covered accounts” must develop and implement a written Identity Theft Prevention Program to detect “red flags” that indicate possible identity theft. The Red Flags Rule requires that a provider’s Identity Theft Prevention Program do the following:

1. Identify relevant red flags for the provider’s covered accounts;
2. Establish procedures to detect those red flags in the provider’s day-to-day operations;
3. Establish the responses to red flags to prevent and mitigate identity theft; and
4. Describe how the provider will keep its Program current and educate staff about the Program.

Examples of red flags relevant to health care providers include the following:

¹ *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, Federal Trade Commission, available at <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm>.

1. Suspicious documents, such as documents provided for identification that appear to have been altered or forged;
2. Suspicious personal identifying information, such as inconsistencies between a social security number range and a date of birth;
3. Suspicious activity related to the covered account, such as mail being returned from the customer's address as undeliverable even though the patient continues to appear for scheduled appointments; and
4. Notices from victims of identity theft, law enforcement authorities or other entities suggesting possible identity theft.

After identifying potential red flags relevant to the provider's practice, the Identity Theft Prevention Program should next describe procedures for detecting these red flags in day-to-day operations. Healthcare providers should review their practices for opening new patient accounts, for accessing patient accounts, and for authenticating existing patients' accounts to appropriate procedures for detecting possible red flags. If a healthcare provider has previously implemented programs to monitor and identify behaviors that indicate identify theft in order to comply with HIPAA or other regulations, those existing procedures can be incorporated into the Identity Theft Prevention Program.

The Identity Theft Prevention Program should outline how employees should respond to red flags. For example, if a new patient presents inconsistent personal identifying information, or personal identification documents that appear forged or altered, what steps should be taken in response? Obviously, the appropriate response will depend on the specific situation and circumstances, and the response may range from requesting additional documentation to not providing services until the discrepancy is resolved.

The Red Flags Rule requires that the Identity Theft Prevention Program be approved by the healthcare provider's board of directors or an appropriate senior level management employee, if the provider does not have a board of directors. Additionally, the Red Flags Rule requires that the board of directors or other designated senior management level employee be involved in the "oversight, development, implementation and administration" of the Program. The provider must also train is staff and employees as necessary to implement the program.

In addition, a qualifying healthcare provider must exercise "appropriate and effective oversight" of any service providers. If a provider outsources services that are covered by the rule, such as opening or managing accounts, collecting debts, handling billing, those service providers must also apply the same standards that the provider would apply in administering those services. Finally, the individual responsible for the Program should report at least annually to the provider's board of directors or senior level employee about the Program's effectiveness. This individual should also describe how the Program is being monitored and recommendations for updating the Program.

While there are no criminal penalties for failing to adopt and implement an Identity Theft Prevention Program, a qualifying “creditor” may be subject to monetary penalties. The FTC offers a “How-To Guide” for complying with the Red Flags Rule, and has released a “fill-in-the-blank” form for businesses that is available at www.ftc.gov/redflagsrule.