Red Flags Rule Will Impact Healthcare Providers

Amy K. Fehn
Jeffrey R. Campbell
Wachler & Associates, P.C.

Despite objections by the American Medical Association and other health care provider organizations, the Federal Trade Commission (the "FTC") has steadfastly maintained that most health care providers will need to comply with the "Red Flags Rule" which is set to go into effect August 1, 2009.

The "Red Flags Rule" is a set of regulations jointly developed by the FTC, the Federal bank regulatory agencies, and the National Credit Union Administration to curb the incidence of identity theft. The regulations were published in the Federal Register on November 9, 2007 and were promulgated to implement section 114 of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act). The compliance date for the Rule was originally set for November 1, 2008 and has been extended twice, in part, because certain industries, including the health care industry, were unaware of their obligations pursuant to the Rule.

The Rule applies to "creditors" and while health care providers do not generally consider themselves to be "creditors", they do meet the rule's broad definition. The Red Flags Rule defers to the definition of "creditor" under the Fair Credit Reporting Act (FCRA) which in turn incorporates the definition from the Equal Credit Opportunity Act (ECOA) and includes "any person who regularly extends, renews, or continues credit" or "any person who regularly arranges for the extension, renewal or continuation of credit." "Credit" is defined by the ECOA as "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore."

The FTC has broadly interpreted the definition of creditor to include any health care provider who regularly bills patients after completion of services, allows patients to set up payment plans, or helps patients get credit from other sources. So, for example, if a health care provider sees a patient, submits the bill to insurance and then bills the patient for any remaining balance resulting from co-payments or deductibles, the health care provider would meet the definition of "creditor" pursuant to the Red Flags Rule.

There are several situations where the FTC has acknowledged that health care providers would not be considered a creditor, including situations where the health care provider always collects full payment prior to rendering any services or where the health care provider only accepts direct payment from Medicaid or other programs that pay in full with no co-payments or deductibles for which the patient is responsible. Also, the mere acceptance of credit cards as a form of payment will not cause a health care provider to be viewed as a "creditor".

It is also important to note that the Rule applies only to "covered accounts". The FTC has broadly defined a "covered account" as including any account for which there is a "reasonable risk" of identity theft. The FTC has specifically stated that it considers patient accounts to bear a "reasonable risk of identity theft" because of increasing concerns about identity fraud in the context of medical care.

Providers who are subject to the Red Flags Rule are required to implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft.

Like the HIPAA Privacy and Security Rules, the Red Flags Rule is flexible and scalable to the size and risk level of the entity. As an example, the FTC notes that small providers with a well known limited patient base will likely have a lower risk of identity theft and could adopt a more limited program than a provider with a larger volume of patients.

Providers who have effective policies in place for compliance with HIPAA Privacy and Security will already meet many of the requirements for the Red Flags Rule with regard to prevention of identity theft. However, in order to be compliant with the Red Flags Rule, providers also need policies specifically dealing with identification, detection and response to "Red Flags" which are defined as "a pattern, practice or specific activity that indicates the possible existence of identity theft."

With regard to medical identity theft, "Red Flags" should include suspicious activities such as:

- Presentation of identification by a patient that looks altered or forged;
- Information provided by a patient that is inconsistent with previous information contained in the medical chart or obtained from another source such as an insurer, e.g., an inconsistent birth date;
- Mail to a patient that is consistently returned as undeliverable even though the patient still shows up for appointments;
- Patient complaints about getting a bill for service that he or she never received;
- Inconsistency between a medical examination and information in the patient's record;
- Notice from victims of identity theft, law enforcement officers or insurers indicating possible identity theft.

To be compliant, an Identity Theft Prevention Program must also be approved by a "board of directors" or a senior management member in the case of entities without a board, and must include staff training and appropriate oversight.

Violation of the Red Flags Rule can result in civil penalties of up to $2,500 per violation and can also damage a provider's reputation and expose them to additional theories of liability. Thus, providers should not delay in beginning to implement a Red Flags Rule compliant Identity Theft Prevention Program. In addition to implementing new policies specifically designed to detect and respond to "Red Flags", providers should review their

HIPAA Privacy and Security Policies to determine the extent to which they address the prevention of identity theft and can be incorporated into an Identity Theft Prevention Program.

AMY K. FEHN is a health care attorney at Wachler & Associates, P.C. Ms. Fehn is a former registered nurse who has been counseling healthcare providers for the past eleven years on regulatory and compliance matter such as HIPAA, Stark, Fraud & Abuse and the defense of RAC and other Medicare and Third Party Payor Audits. She can be reached at (248) 544-0888 or afehn@wachler.com.

JEFFREY R. CAMPBELL is a health care attorney at Wachler & Associates, P.C., where he specializes in transactional and corporate matters; compliance; audit defense; reimbursement and contracting matters; and staff privilege and third party payor de-participation matters. He can be reached at (248) 544-0888 or at jcampbell@wachler.com.