EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *March 2009*

New "Red Flag" Identity Theft Rules Apply to Healthcare Providers

Physicians, hospitals and other healthcare providers may not be aware that the federal Red Flag Rules, 16 C.F.R. § 681 (the "Rules"), may apply to them. The Rules, which become effective on May 1, 2009, require covered entities to formally address the risks of identity theft and develop a plan to prevent such risks.

Eric D. Fader, Counsel

Socheth Sor, Associate

The Rules have been widely overlooked by healthcare providers because they were promulgated under the Fair and Accurate Credit Transaction Act of 2003 by federal agencies that regulate financial institutions and, thus, appear to apply only to financial institutions. However, the Federal Trade Commission (the "FTC") has made clear that the Rules are applicable to healthcare providers that allow their patients to defer payment for the professional services they receive.

When is a Healthcare Provider Covered by the Red Flag Rules?

The Rules will apply to a healthcare provider if it is a "creditor" with "covered accounts." Under the Rules, "creditor" is defined to mean:

(i) Any person who regularly extends, renews, or continues credit;
(ii) Any person who regularly arranges for the extension, renewal, or continuation of credit; or
(iii) Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

According to the FTC, a healthcare provider may be considered a creditor if it extends credit to patients by offering them extended payment plans and by billing in arrears for medical treatment.

If you meet the definition of creditor, the next step is to determine whether you offer or maintain any covered accounts because the Rules only apply if you do. The Rules define "covered account" as follows:

(i) An account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, such as a credit card account . . . ; and
(ii) Any other account 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, including financial, operational, compliance, reputation, or litigation risks.

16 C.F.R. § 681.2(3).

The definition of covered accounts is broad. The FTC does not provide examples for the second part of the definition of "covered account" because the determination of whether an account falls within this second definition involves a case-by-case, risk-based analysis. Whether an account is a covered account will depend on the perceived vulnerability of the accounts to identity theft.

Healthcare providers maintain various types of records for which there is a "reasonably foreseeable risk" of identity theft, including patient financial and medical information. For example, a patient billing account may be a covered account under the first part of the definition of "covered accounts" if the health care organization permits payments in installments or extensions of time to pay. It will also be a covered account under the second part of the definition because there is a reasonably foreseeable risk that personal information maintained in connection with the account is vulnerable to identity theft.

Due to the breadth of the definitions, each healthcare provider should determine whether it offers or maintains covered accounts. The onus is on each healthcare provider to determine whether it is subject to the Rules and required to establish a Program (as defined below).

How to Comply with the Red Flag Rules

If you determine that you are a creditor under the Rules, you must develop and implement a written Identity Theft Prevention Program ("Program") to detect, prevent, and mitigate identity theft in connection with your patients' billing and medical records. Specifically, the Program must contain policies and procedures to:

- Identity relevant patterns, practices and specific forms of activity that are Red Flags signaling possible identity theft;
- Detect Red Flags;
- Respond appropriately to Red Flags; and
- Ensure that the Program is updated periodically to reflect changes in risk.

To administer the Program, you must:

- Obtain approval of the Program by your board of directors;
- Train your staff in the Program's procedures; and
- Exercise oversight of arrangements with third-party service providers.

Healthcare providers now have less than two months to comply with the Rules. It's not too late to develop or revise your existing security policies to comply by May 1, 2009, but you should start now.

If you would like assistance in establishing a Program, contact Eric Fader at 212.912.2724.

If you determine that you are a creditor under the Rules, you must develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with your patients' billing and medical records.

This advisory is for guidance only and is not intended to be a substitute for specific legal advice. If you would like further information, please contact the Edwards Angell Palmer & Dodge LLP attorney responsible for your matters or one of the attorneys listed below:

Eric D. Fader, Counsel 212.912.2724 efader@eapdlaw.com
Socheth Sor, Associate 860.541.7773 ssor@eapdlaw.com

Edwards Angell Palmer & Dodge

111 Huntington Avenue
Boston, MA 02199
Tel 617.239.0100
Fax 617.227.4420
eapdlaw.com