Foster Garvey

Summary of the Red Flags Rule

Legal Alert
April 22, 2009

Garvey Schubert Barer Legal Update, April 22, 2009.

Statutory Authority: Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

Statutory Requirements: Requires creditors who maintain covered accounts to establish a written identity theft prevention program to prevent identity theft in their practices.

Compliance Deadline: November 1, 2008. However, enforcement of the rule is suspended until August 1, 2009.

Definitions

Creditor: any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in a decision to extend, renew, or continue credit.

- FTC interprets this definition to include healthcare providers if that health care provider does not regularly demand payment in full for services at the time the services are rendered.
- FTC states that this definition also includes healthcare providers who bill a patient's insurance company before requesting payment in full from the patient.

Covered Accounts are accounts that permit multiple payments or transactions and that pose a reasonably foreseeable risk to customers or to the safety and soundness of medical practices from identity theft, including financial, operational, compliance, reputation, or litigation risks.

- The FTC considers patient billing accounts to be "covered accounts."

Identity Theft Prevention Program: A program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account, and must be appropriate to the size and complexity of the medical practice and the nature and scope of its activities.

- The written identity theft program must be approved by the Board of Directors or, if not Board, Senior Management.

Identity theft means a fraud committed or attempted using identifying information of another person without authority.

Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. Includes, but is not limited to:

- Name, SSN, DOB, driver's license number, alien registration number, passport number, employer or taxpayer ID number;
- Unique biometric data such as fingerprints, voice prints, etc.;
- Unique identification number, address, or routing code; or
- Telecommunication identifying information or access device.

A **Red Flag** is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Goals of an Identity Theft Protection Program

An identity theft protection program should have five goals:

1. Identify relevant indicators of a possible risk of identity theft (Red Flags)
2. Detect Red Flags
3. Respond to Red Flags in order to prevent and mitigate identity theft
4. Update the program periodically
5. Properly administer the program

Examples of Red Flags

The FTC lists 26 examples in 5 categories. Some of the FTC examples that would appear applicable to healthcare providers include:

Areas of concern identified in alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection agencies.

Presentation of suspicious documents.

- Documents appeared to be forged or altered
- Photograph presented is not consistent with the appearance of the person presenting
- Information on documentation presented is not consistent with readily accessible information.

Presentation of suspicious personal identifying information.

- Personal identifying information provided is not consistent with external information sources.

Unusual use of, or suspicious activity related to, a covered account.

- Mail addressed to patient is returned repeatedly as "undeliverable."
- You are notified that the patient is not receiving paper account statements.

Notice from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with a covered account held by the healthcare

provider.

- Advised by patient that someone has been opening accounts in their name.

Detecting Red Flags

Have appropriate staff verify information received from patients.

Require identifying information including government issued identification.

Verify information where possible.

Respond to Red Flags

Request additional identifying information when necessary.

Monitor covered accounts more closely if suspicious.

Contact patient if concerned and tell patient of concern.

Close account.

Notify law enforcement.

Determine that no response is warranted. (Will probably want to document the reason why no response is warranted).

Updating the Identity Theft Protection Program

Identify a person or group by title who is charged with the responsibility to periodically review the effectiveness of the Identity Theft Prevention Program.

Identify a person or group who is charged with responsibility of developing, implementing, and administering your Identity Theft Prevention Program.

Implementation

The FTC expects that all healthcare providers who maintain covered accounts will create and implement an Identity Theft Protection Program and put the policy into actual practice within the organization.

The FTC does *not* expect healthcare providers to spot every case of identity theft or apprehend every identity thief

The FTC recognizes that healthcare providers are organizations to provide healthcare and are *not* an investigatory / detective / law enforcement agency.

Additional information regarding the Red Flags Rule is available at www.ftc.gov/redflagsrule.