

MARCH 2009

Red Flag Rules Now In Effect for Physicians; Enforcement to Begin May 1, 2009

By: Jackie M. Crain and
Michael A. Igel, Trenam Kemker
Health Law Team,
St. Petersburg, Florida

Overview

Physicians and physician groups may be unaware that they have a looming deadline for compliance with complex new federal regulations. The Federal Trade Commission (“FTC”) and other federal agencies issued a set of rules that require “financial institutions” and “creditors” holding consumer or other “covered” accounts to develop and implement an identity theft prevention program that complies with the regulations by November 1, 2008. The FTC subsequently postponed enforcement of these rules until May 1, 2009 to allow those who fall under its purview to achieve compliance. These rules, commonly referred to as the Red Flag Rules (the “Rules”), affect individual physicians, physician groups, hospitals and other health care organizations that qualify as “creditors” based upon billing and collection practices. The new regulations provide guidelines for identifying patterns, practices and specific forms of activity – in short, red flags – that indicate the possible existence of identity theft.

Why is My Practice Affected?

On its face, the Rules were easy for physicians to overlook because they seem aimed at creditors such as banks, credit unions, credit

card companies, auto dealers and other creditors that utilize sensitive personal information about a customer. Moreover, the Rules were issued jointly by various entities that regulate financial institutions (such as the FTC, FDIC, and OCC). However, the Rules are not so limited, and because “creditors” under the Rules is defined broadly, even health care providers must comply.

The American Medical Association (“AMA”) challenged the FTC’s position that the Rules should apply to physicians in a September 30, 2008 letter to the FTC. On February 4, 2009, the FTC responded to the AMA’s letter and reiterated that physicians are indeed “creditors” under the Red Flag Rules.

Who is a “creditor” and What are The Red Flag Rules Penalties?

The Rules define a “creditor” as “any business or person who arranges for the extension, renewal or continuation of credit” with a “covered account.”

A “covered account” is defined as either (1) an account primarily for personal, family or household purposes that is designed to permit multiple transactions, or (2) any other account for which there is a foreseeable risk to customers of the safety and soundness of the creditor from identity theft.

Most physicians and group practices fall under the FTC’s definition of a creditor because they generally do not collect payment at the time a service is rendered and often hold off billing patients in full. Routine practices such as setting up a payment plan or billing an insurance company before charging the patient fall under the ambit of the Rules. Moreover, any kind of patient account or payment plan that involves multiple transactions or multiple payments is also subject to the Rules. Notably, the FTC has stated that if there is not a full payment at the time of services, it is a credit transaction. This includes payment of copayments and deductibles that are the obligation of the patient.

An identity theft event such as a data breach or a disgruntled employee reporting non-compliance to the FTC could subject a physician’s practice to monetary penalties and civil litigation. Creditors, such as physicians, must be concerned with three enforcement mechanisms:

- *Federal Enforcement* – The FTC is authorized to bring enforcement actions in federal court for violations, and could enact penalties of up to \$2,500 per violation of the Rules;
- *State Enforcement* – The Rules authorize states to bring actions

continued on back page

Red Flag Rules continued

on behalf of their residents and recover up to \$1,000 per violation, in addition to recovery of attorney's fees; and

- *Civil Liability* – Each consumer (patient) may be entitled to recover actual damages sustained from a violation.

Checklist for Working Toward Compliance with the Red Flag Rules

Although no two practices are exactly alike, we have included below a checklist that can be used as a starting point for compliance with the Red Flag Rules.

- ☐ Recognize that HIPAA is no longer the only federal law that governs your protection of sensitive data and appoint a person to review the Red Flag Rules and lead compliance efforts.
- ☐ Review the 26 example red flags and identify which of them is relevant to your practice and processes ([available at http://edocket.access.gpo.gov/cfr_2008/janqtr/16cfr681AppA.htm](http://edocket.access.gpo.gov/cfr_2008/janqtr/16cfr681AppA.htm)).
- ☐ Identify employees who are involved in verifying the identity of patients and “admitting” them to the practice as they arrive. Involve these employees in the review of red flags and

development of a compliance plan.

- ☐ Create a procedure for detecting when red flags occur in your practice.
- ☐ Develop a policy that outlines how your practice will respond when red flags are detected. The policy and procedure should be appropriate to the size and complexity of the practice and its activities.
- ☐ Set an internal deadline for reviewing the policy and procedure to ensure that the program is updated periodically to reflect changes in risks.

☐ Document approval of the new red flags policy and procedure by the Board of Directors or a committee thereof.

☐ Train staff, as necessary, to effectively implement the policy and procedure.

As burdensome as the Rules seem, they carry with them an important business and compliance purpose, and the sanctions for violation can be severe. Ideally, these new policies and procedures will supplement your practice's HIPAA compliance efforts and enhance patient confidence in your practice's concerns for protecting data and avoiding identity theft events.

Because patient intake and record retention systems differ from one medical practice to another, it is important to have a Red Flag Rules compliance plan that is tailored specifically to your practice. You may have questions about the Red Flag Rules or need assistance implementing a compliance program or finalizing policies and procedures.

Contact us if you need additional assistance.

Don B. Weinbren
Tel: 813-223-7474
E-Mail: dweinbren@trenam.com

Richard O. Jacobs
Tel: 727-896-7171
E-Mail: rjacobs@trenam.com

L. Jim Dickson
Tel: 727-896-7171
E-Mail: jdickson@trenam.com

Jacqueline Myles Crain
Tel: 727-896-7171
E-Mail: jcrain@trenam.com

Douglass Farnsworth
Tel: 813-227-7455
E-Mail: dfarnsworth@trenam.com

Michael Igel
Tel: 727-820-3963
E-Mail: migel@trenam.com

Trenam, Kemker, Scharf, Barkin, Frye, O'Neill & Mullis

TAMPA OFFICE Bank of America Plaza, 101 East Kennedy Boulevard, Suite 2700, Tampa, FL 33602, Phone 813-223-7474

ST. PETERSBURG OFFICE Bank of America Tower, 200 Central Avenue, Suite 1600, St. Petersburg, FL 33701, Phone 727-896-7171

www.trenam.com