

**FTC Red Flags Rule**

Physician Practice Clients

March 10, 2009

D. Brent Wills, Esquire

Pursuant to regulations recently adopted by the Federal Trade Commission (the “FTC”), beginning as of May 1, 2009, many physician practices and other health care providers will be required to have in place written policies and procedures to protect against identity theft. Representatives of the health care industry have vigorously lobbied and debated the FTC to exclude physician practices and other health care providers from the scope of these so-called “Red Flags Rule.” The FTC, however, has consistently held to an expansive application of the rules. Most recently, the FTC, in response to lobbying efforts by the American Medical Association (“AMA”) and other organizations, indicated that physicians who regularly bill their patients for services rendered (including copayments and coinsurance) must comply with the Red Flags Rule.¹

In response to these developments, every physician practice should:

1. *Confirm that the practice is subject to the Red Flags Rule*

A physician practice is subject to the Red Flags Rule if it is a “creditor” that has “covered accounts,” within the meaning of the rules. Assuming the FTC will not waver from its broad application of the rules, any physician practice that accepts payment from patients other than in full in advance or immediately upon the rendering of medical services should prepare to comply with the Red Flags Rule.

2. *Conduct a Risk Assessment to Identify Potential “Red Flags” for Identity Theft*

The practice should appoint an appropriate individual (for example, a compliance officer / manager) to examine (i) the practice’s patient accounts to determine whether,

¹See Letter dated February 4, 2009 from Eileen Harrington, Office of the Director of Bureau of Consumer Protection, Federal Trade Commission, to Margaret Garikes, Director of Federal Affairs, American Medical Association, available at <http://www.ftc.gov/os/statutes/redflags.pdf>; see also Memorandum of Michael D. Maves, Executive Vice President and CEO of the American Medical Association dated February 6, 2009, available at <http://files.e2ma.net/16424/assets/docs/2-6-09finalmemotofederation1.pdf>. Other published FTC guidance indicates that health care providers are subject to the Red Flags Rule if (i) “they bill consumers after their services are completed;” or (ii) “the consumer ultimately is responsible for the medical fees.” See *The “Red Flags” Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identify Theft*, available at <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>.

and under what circumstances, such accounts may be vulnerable to identity theft; and (ii) the practice's current policies and procedures for handling and authenticating patient identification information (for example, policies and procedures for HIPAA compliance) to determine whether they satisfy the Red Flags Rule. In particular, the practice should determine whether it has policies and procedures in place to identify, detect and respond to (see below) certain specific categories of "red flags" identified by the FTC, namely (i) receipt of alerts, notifications or other warnings received from third parties with regard to a patient (for example, consumer reporting agencies or service providers); (ii) presentation by a patient of suspicious identification documents (for example, invalid social security number, forged driver license) or information (for example, suspicious change of address); (iii) unusual use of, or other suspicious activity related to, a patient's payment, insurance or other financial information; and (v) receipt of notification regarding possible identity theft.

3. Develop Written Policies and Procedures to Comply with the Red Flags Rule

If the practice determines that its current HIPAA and other policies and procedures do not satisfy the Red Flags Rule, the practice must, to the extent necessary to comply, prepare and adopt written policies and procedures (an "Identify Theft Prevention Program," in FTC parlance, herein, the "Program") that (i) identify potential "red flags" for identity theft targeted in the examination conducted by the practice (see above); (ii) detect a red flag, if and when it occurs; (iii) respond appropriately to prevent or mitigate identity theft, in the event a red flag is detected; and (iv) ensure the Program is periodically updated to reflect the practice's experience with identity theft, any changes in potential methods of identity theft, and other relevant factors.

4. Administer the Program in Compliance with the Red Flags Rule

The Program must be approved by the practice's board of directors or an applicable committee of the board. Moreover, once the Program is in place, the board of directors or an appropriate, duly authorized officer (for example, the compliance officer) must be responsible for continuing oversight, development, implementation and administration. This includes coordinating staff training and monitoring service provider arrangements, including confirming, in the event that service providers handle information that may be subject to identify theft, that such providers have policies and procedures in place that comply with the Red Flags Rule.

The above merely provides an overview of the application and requirements of the Red Flags Rule. There are many additional factors, and considerable additional FTC guidance, that may impact whether a particular physician practice is subject to the Red Flags Rule and, if so, the particular methods whereby the practice may comply with the rules. If your physician practice needs assistance to determine whether it is subject to the Red Flags Rule and what it must do to comply, please contact us at (334) 244-1111.