



Red Flag Compliance for Healthcare Providers

02.11.09

On November 9, 2007, the Federal Trade Commission (FTC), in conjunction with other agencies, published the “Red Flag Rules” identifying the steps that a creditor or financial institution must take in order to implement an Identity Theft Prevention Program to define, detect and respond to Red Flags to prevent or mitigate identity theft. A “red flag” is a suspicious circumstance that should prompt the financial institution or creditor to be alert for possible identity theft.

The FTC’s staff attorneys have broadened the application of the Red Flag Rules to the health care arena through their designation of certain physicians and physician groups as “creditors”. Specifically, under the FTC’s interpretation, most physicians and group practices likely fall under the definition of “creditor” because they generally do not require full payment at the time they see patients and often hold off billing patients in full. Although accepting credit card payments does not apply in this case, routine practices such as setting up a payment plan or billing an insurance company before charging the patient likely do, especially if the patient is ultimately responsible for medical fees, including co-pays, deductibles or non-covered services.

A physician or group practice that qualifies as a creditor and that offers or maintains covered accounts (i.e. an account involving a “foreseeable” risk of identity theft, which, for physicians, means most billing accounts) must develop and implement a written Identity Theft Prevention Program that, at a minimum, (1) is adopted by the owners, board of directors or other governing body, (2) is designed to identify, detect and respond appropriately to Red Flags, (3) is updated periodically to reflect changes in risks from identity theft, (4) designates responsibility for the program at the senior management level, and (5) provides staff training and effective oversight.

Compliance with the Red Flag Rules is “scalable” depending on the size of the organization (i.e. a single physician practice would not need to implement the level of Identity Theft Prevention Program that a twenty physician practice would implement). Therefore, the Red Flag Rules give flexibility to organizations to implement a program that best suits their business. While the development and implementation of an Identity Theft Prevention Program will involve time and expense, the level of time and expense will depend in large part upon the ability to build off of procedures and compliance plans already in place to protect patients’ protected health information under HIPAA.

The FTC and other experts have identified examples of “red flags” in the healthcare setting, including:

- (a) a complaint or question from a patient based on the patient’s receipt of a bill for another individual; a bill for a product or service that the patient denies receiving; a bill from a health care provider that the patient never patronized; or an Explanation of Benefits or other notice for health services never received;
- (b) records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient, i.e. substantial discrepancies in age, race, and other physical descriptions;
- (c) a complaint or question from a patient about the receipt of a collection notice from a bill collector;
- (d) a patient or insurance company report that coverage for legitimate hospital stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached;
- (e) a complaint or question from a patient about information added to a credit report by a health care provider or insurer;
- (f) a dispute of a bill by a patient who claims to be the victim of any type of identity theft;

- (g) a patient who has an insurance number but never produces an insurance card or other physical documentation of insurance; and/or
- (h) a notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

Upon identifying a red flag, a physician or group practice must have a plan for evaluating whether identity theft has occurred and how to mitigate its effects. The FTC guidance states that appropriate responses may include: (i) monitoring a covered account for evidence of identity theft; (ii) contacting the patient; (iii) changing any passwords, security codes or other security devices that permit access to a covered account; (iv) reopening a covered account with a new account number; (v) not opening a new covered account; (vi) closing an existing covered account; (viii) not attempting to collect on a covered account or not selling a covered account to a debt collector; (ix) notifying law enforcement; and/or (x) determining that no response is warranted under the particular circumstances.

On or prior to May 1, 2009, physicians, physician groups and other health care entities that qualify as “creditors” under the Red Flag Rules must implement an Identity Theft Protection Program in compliance with the requirements set forth herein and elsewhere within the Red Flag Rules. Failure to comply with the Red Flag Rules can result in civil money penalties for each violation, regulatory enforcement action, and negative publicity. In addition, although the Red Flag Rules do not allow for any private legal action in the event of a violation, there is still the potential for private lawsuit under state law because a violation of the Red Flags Rules may itself be a violation of state laws, which laws may permit actions by consumers or the state attorney general.

Physicians and physician groups should seek legal counsel regarding compliance as making the required changes or implementing the required programs may be difficult. If you have any questions regarding this Alert, or would like assistance in developing and implementing an Identity Theft Protection Program, please contact Attorney Jason F. Haupt (jhaupt@kwgd.com) or Attorney Michael J. Bogdan (mbogdan@kwgd.com) at (330) 497-0700.

NOTE: This general summary of the law should not be used to solve individual problems since slight changes in the fact situation may require a material variance in the applicable legal advice.
