

RATH YOUNG PIGNATELLI

National Impact. Uniquely New Hampshire.

Red Flags Rule — Update for Health Care Providers

Identity Theft Program Required By May 1, 2009

March 17, 2009

Clarification by the Federal Trade Commission

The FTC's Red Flags Rule requires "creditors" to implement written identity theft policies and procedures. While there was some initial uncertainty regarding the extent to which physician practices and other health care providers would be subject to the Rule, the FTC has now made it clear that ordinary billing and collection practices are sufficient to render physician practices "creditors" for the purpose of the Rule.

In a recent letter to the AMA, the FTC stated that physician practices are considered "creditors" if they regularly defer payment for services, *for example* by submitting a claim to an insurance carrier first and then billing any remaining unpaid amounts to the patient. Thus, many physician practices and other providers will find themselves subject to the Red Flags Rule.

When is a Health Care Provider Covered by the Rule?

A physician practice or other health care provider that is a "creditor" and that maintains "covered accounts" is subject to the Red Flags Rule.

A "covered account" includes an ongoing physician/patient relationship that is designed to permit multiple payments or transactions or for which there is a reasonably foreseeable risk of identity theft; the last part of the definition will capture most patient medical records, because of the personal identifying and financial information they contain.

Obligations Under the Red Flags Rule — General

The Red Flags Rule requires a creditor that maintains covered accounts to develop and implement a written identity theft program that has reasonable policies and procedures to:

- *Identify* red flags (a red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft);
- Detect red flags; and
- Respond *appropriately* to any red flags that are detected.

Red flags that might arise in a health care context, where medical identity theft is a real concern, include:

- A patient has an insurance number but is unable to produce an insurance card or other physical documentation of insurance;
- Suspicious documents, for example, documents presented for identification that appear to have been altered or forged;
- Suspicious personal identifying information, including suspicious changes of address;
- A complaint or question from a patient based on the patient's receipt of:
 - * A bill for another individual;
 - * A bill for services that the patient denies receiving;

- * A notice of insurance benefits for health care services never received; and
- A dispute of a bill by a patient who claims to be the victim of identity theft.

Appropriate responses to a red flag that is detected may include such things as:

- Monitoring a covered account for evidence of identity theft;
- Contacting the patient;
- Changing any passwords that permit access to the covered account;
- Not opening a covered account;
- Not attempting to collect on a covered account;
- Notifying law enforcement; and
- Determining that no response is warranted in the circumstances.

In determining an appropriate response, the provider should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to the patient's records.

Providers should bear in mind that the risk of identity theft comes not just from outside the organization, but also from *inside* the organization.

Guidelines on developing an identity theft program, as well as additional sample red flags, are contained in an appendix to the Red Flags Rule, and in a paper published by the World Privacy Forum ([see](#) links below).

A health care provider's identity theft program must be approved initially by the entity's board of directors (or an appropriate committee of the board), and must be updated periodically. The board or committee must remain involved in the oversight and administration of the program. The health care provider must provide appropriate training for its staff.

What Sort of Identity Theft Program is Required for Most Physician Practices and Providers?

The FTC has signaled that the Red Flags Rule should not impose significant burdens for most providers. The Red Flags Rule is designed to be flexible, and requires simply that an identity theft program be tailored to the degree of identity theft risk faced by the particular provider. According to the FTC, this risk may in most cases be minimal or non-existent, so that a streamlined program would be adequate.

For example, the FTC suggests that for most physicians in a low risk environment, an appropriate program might consist of checking photo identification at the time services are sought, and having appropriate procedures in place in the event the practice is notified that a patient's identity has been misused. Appropriate procedures might include not trying to collect the debt from the real patient, and ensuring that any information about the identity thief is maintained separately from information about the real patient.

Recommended Action for Physician Practices and Other Health Care Providers

With the deadline for compliance less than two months away (May 1, 2009), physician practices and other health care providers should take immediate steps to determine whether or not they are subject to the Red Flags Rule. If they are subject to the Rule, they should, as soon as possible, begin to develop an identity theft program, either as a standalone program or as part of their HIPAA policies and procedures.

Both the appendix to the Red Flags Rule and the World Privacy Forum paper are helpful resources. In addition, there is a possibility that physician organizations such as the AMA may develop model policies for their members; we note that the FTC has offered to help the AMA in assisting physicians to comply with the Red Flags Rule in the "least burdensome" way possible.

In the meantime, physician practices and other health care providers are encouraged to contact their legal counsel with any questions.

Helpful Links

To review our October 30, 2008 E-Mail Alert on the Red Flags Rule, please [click here](#).

For the FTC's February 4, 2009 letter to the AMA, please [click here](#).

For the Red Flags Rule, please [click here](#) or see 16 CFR Part 681.

For a copy of the World Privacy Forum paper "Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers," please [click here](#).

For more details please contact Barbara Greenwood at bjg@rathlaw.com or Lucy Hodder, Chair of the Healthcare Practice Group at lch@rathlaw.com or by calling 603.226.2600.

*This information should not be construed as legal advice
or relied upon to resolve legal problems.*