

RATH YOUNG PIGNATELLI

Privileged and Confidential

MEMORANDUM

FROM: Lucy C. Hodder
Barbara J. Greenwood

DATE: April 1, 2009

RE: Red Flags Rule

We are advising our health care clients to be aware of the heightened risk of medical identity theft given the current economic climate. In order to assist you in protecting against the risk of identity theft and complying with the FTC's Red Flags Rule, we have prepared the following summary of the steps that health care providers should take to comply with the Red Flags Rule. The deadline for compliance is May 1, 2009.

We would be pleased to provide any further assistance you require, review your draft policies, and/or provide training.

As a preliminary matter, of course, a provider should determine whether it is in fact subject to the Rule:

A. Preliminary Step: Confirm that the Red Flags Rule applies

1) Confirm that you are a "creditor"

Do you regularly defer payment for services? For example, do you regularly permit patients to enter into payment plans for services already received? Or, do you submit claims to insurance carriers first, and then bill any remaining unpaid amounts to the patient? Unless you provide services only on a prepaid basis, you are probably a creditor.

2) Confirm that you maintain "covered accounts"

A "covered account" includes an ongoing physician/patient relationship designed to permit multiple payments or transactions, or for which there is a reasonably foreseeable risk of identity theft. Most patient medical records will be captured by this definition.

Only providers who are "creditors" and who maintain "covered accounts" are required to develop a written identify theft program, to *identify, detect* and *respond* to possible risks of identity theft.

B. Next: Develop a Written Identity Theft Program ("Program")

RATH YOUNG PIGNATELLI

Privileged and Confidential

1. General

The Red Flags Rule is flexible. Your Identity Theft Program need only address any reasonably foreseeable risks of identity theft relevant to you. If you identify only minimal risks of identity theft, your Program can be very simple.

But, in assessing your risks and developing your Program, you must follow the steps called for by the Red Flags Rule.

2. Step One: Assess your risk for identity theft

Identify any reasonably foreseeable risks for identity theft that exist in your practice, taking into account:

- 3) *The types of covered accounts that you maintain.* For example, do your patient's medical and billing records contain personal information about the patient that could be used by an identity thief, such as insurance information, SSN, drivers' license, and any other personal identifying information?
- 4) *Your methods for opening covered accounts.* For example, do you have adequate procedures in place to verify a patient's identity? Is there a risk that a patient could obtain medical services by pretending to be someone else?
- 5) *How you provide access to covered accounts.* For example, do you have adequate procedures to verify a patient's identity before releasing information from their medical records to them, or before implementing a change of address request? Do you have adequate protections in place to protect patient information from *internal* identity theft, such as password-protected access on a need-to-know basis? Do you have policies prohibiting employees from taking laptops containing unencrypted patient information offsite? Do you perform background checks before hiring new employees?
- 6) Any previous experiences the practice has had with identity theft.

RATH YOUNG PIGNATELLI

Privileged and Confidential

3. Working Group

We recommend that you create a working group to perform the above assessment and to develop the necessary policies and procedures (described below). Consider including the business manager, admissions/intake staff, billing staff, and, if you have one, an IT person, in the working group.

4. Step Two: Identify Red Flags

Identify relevant red flags for your “covered accounts.” Red flags are patterns, practices, or specific activities that indicate the possible existence of identity theft. These should be based on your assessment of your risks for identity theft.

In identifying red flags, the Red Flags Rule requires that you consider the sample red flags that are listed in Appendix A to the Rules (copy attached). While many of such sample red flags are relevant for financial institutions and not for health care providers, red flags that might arise in a health care context (where medical identity theft is a real concern) include:

- 7) A patient has an insurance number but is unable to produce an insurance card or other physical documentation of insurance;
- 8) Suspicious documents, for example, documents presented for identification that appear to have been altered or forged;
- 9) Suspicious personal identifying information, including suspicious changes of address;
- 10) 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
- 11) A dispute of a bill by a patient who claims to be the victim of identity theft.

5. Step Three: Develop Policies and Procedures to Detect Red Flags

The Red Flags Rule requires that you develop appropriate policies and procedures to *detect* the red flags that you have identified, both in connection with opening covered accounts (i.e., new patients) and with existing covered accounts (i.e., existing patients).

Such policies might include, for example: for new patients, obtaining identifying information about, and verifying the identity of, the patient; and for existing patients, authenticating their identity, and verifying the validity of any change of address requests.

Some providers may choose to check drivers’ licenses or even copy them. Providers in New Hampshire should be aware that RSA 263:12 prohibits the copying and scanning of a photo license. The statute is set forth below. The Department of Safety, however, will permit providers who maintain and implement a HIPAA privacy policy protecting the personal

RATH YOUNG PIGNATELLI

Privileged and Confidential

information, to copy a driver's license or photo ID if: (1) the patient consents; and (2) the copy is can not be mistaken as an ID, and thus is in black and white or otherwise marked as a copy. If the patient refuses to provide photo ID, alternative options should be considered.

263:12 Prohibitions. – It shall be a misdemeanor for any person to: ...

VII. Photograph, photostat, duplicate, or in any manner reproduce any license to drive a motor vehicle or facsimile thereof in such a manner that it could be mistaken for a valid license, or have in his possession any such photograph, photostat, duplicate, reproduction or facsimile unless specifically authorized by the director.

VIII. Manufacture, advertise for sale, sell, or possess any fictitious, facsimile or simulated non-driver's identification card provided under RSA 260:21.

IX. Photograph, photostat, duplicate, or in any manner reproduce any official non-driver's identification card or facsimile thereof, in such a manner that it could be mistaken for a valid identification card issued under RSA 260:21, or have in his possession any such photograph, photostat, duplicate, reproduction or facsimile unless authorized by the director.

X. Knowingly scan, record, retain, or store, in any electronic form or format, personal information, as defined in RSA 260:14, obtained from any license, unless authorized by the department. Nothing in this paragraph shall prohibit a person from transferring, in non-electronic form or format, personal information contained on the face of a license to another person, provided that the consent of the license holder is obtained if the transfer is not to a law enforcement agency. Notwithstanding any other provision of law, any person selling alcohol or tobacco who uses due diligence in checking identification to prevent unauthorized sales and purchases of alcohol and tobacco shall not be held responsible for the acceptance of fraudulent identification. Where due diligence is exercised on the part of the seller, the unauthorized purchaser shall be liable for any penalty or fine resulting from the unauthorized sale.

We recommend that you start by having your working group review your existing HIPAA policies and procedures. Depending on their level of detail, your HIPAA privacy and security policies may already incorporate measures that help protect PHI from identity theft. Your red flag policies can build on these. The Rules permit you to incorporate, as appropriate, your existing policies into your Program. You should also review your intake procedures to determine what information regarding patient identification is appropriate to request given the nature of your practice.

6. Step Four: Develop Policies and Procedures for Responding to Red Flags

Your Program must contain policies and procedures for responding appropriately to any red flags that are detected, so as to *prevent* and *mitigate* identity theft. For example, appropriate responses to a red flag that is detected may include such things as:

- 12) Monitoring a covered account for evidence of identity theft;

RATH YOUNG PIGNATELLI

Privileged and Confidential

- 13) Contacting the patient;
- 14) Changing any passwords that permit access to the covered account;
- 15) Not opening a covered account;
- 16) Not attempting to collect on a covered account;
- 17) Notifying law enforcement; and
- 18) Determining that no response is warranted in the circumstances.

(We note that it is unlikely that your existing HIPAA policies incorporate such responses.)

7. Step Five: Obtain Board Approval

Your Program must be approved by your Board or by an appropriate committee of your Board.

8. Step Six: Training

Your Program must provide for your staff to be trained, as necessary, to implement the Program effectively.

9. Continuing Obligations

The Red Flags Rule sets forth a number of continuing obligations for Identity Theft Programs, including:

- Board or Senior Management Oversight

Your Program must provide for the involvement of the Board, an appropriate Board committee, or a designated senior management official, in the oversight, development, implementation and administration of the Program. FTC Guidance suggests that your Program should require a report to the Board/committee/senior manager at least annually.

RATH YOUNG PIGNATELLI

Privileged and Confidential

- Oversight of Service Providers

The Red Flags Rule requires that you exercise appropriate and effective oversight over service provider arrangements, where they involve access to “covered accounts” (for example, arrangements with a third party billing company). FTC Guidance suggests that providers should ensure that the service providers have their own red flags policies in place, to address red flags that might arise in the performance of their services for you. This could be done through the services agreement or the business associate agreement. Another option is to send a letter to all your third party service providers asking them to confirm that they have such red flag policies in place.

- Updates

The Program should be updated periodically.

Developing a simple and workable policy that addresses the risks relevant to your practice should be fairly straightforward, if you follow the approach outlined above. For your assistance, we attach sample policies developed by the American Health Lawyers Association and by the American Hospital Association, which we hope will provide a useful starting point. Of course, we would be happy to help you develop your own red flags policy.

Additional background can be found in our email alerts on the Red Flags Rule, available on our website: www.rathlaw.com.

Attachments: Red Flags Rule
Appendix A
Sample Policies