Publication of Medical Mutual / Professionals Advocate®

DOCTORS Rx

Volume 17, No. 2 Special Edition 2009

A Letter from the Chair of the Board

Dear Colleague:

We are pleased to provide you with this Special Edition of the Doctors RX newsletter featuring the FTC's "Red Flags" Rule. This newsletter will give you practical information regarding what you need to know about compliance and about putting a medical identify theft protection program in place in your practice.

George S. Malouf, Jr., M.D.
Chair of the Board
Medical Mutual Liability Insurance Society of Maryland
Professionals Advocate Insurance Company

FTC Delays Enforcement of "Red Flags" Rule

The Federal Trade Commission (FTC) recently announced a delay in enforcement of the Identity Theft Prevention Policy commonly known as the "Red Flags" Rule until August 1, 2009. So, what are these new regulations and what do health care practices need to have in place in order to be in compliance?

The Red Flags Rule is part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. This federal law requires businesses to recognize the warning signs of identity theft through patterns, practices, and specific activities. The regulation also requires businesses to develop and implement written identity theft prevention programs. The rule first appeared in the Federal Register in November 2007 with a compliance date of November 2008. This first date of enforcement was initially delayed until May of this year and then recently delayed again until August 2009. The American Medical Association and other medical societies have been lobbying the FTC to not include medical practices under the rule. These efforts have been without success, as the FTC has concluded that medical practices are by definition a creditor and therefore must comply with the regulations.

Continued on next page

Jama Allers, CMA-C, CMC
Practice Consultant for the Medical and Chirurgical Faculty of Maryland – The Maryland State Medical Society (MedChi).

So, who must comply with the Red Flags Rule? Health care practices, hospitals, banking institutions and any business that by definition is a creditor must have a written working policy in place. A creditor is defined as any entity that regularly extends, renews or continues credit, including any business that accepts transactions that defer payment of debt or accept deferred payment for products and services. Under this definition, health care practices that accept deferred payments, such as billing insurance carriers and waiting for payment or allowing patients to pay with monthly payment plans for services, are creditors.

As creditors, health care practices should carefully evaluate their covered accounts. The FTC defines a covered account as any account that a creditor offers or maintains used primarily for personal or family purposes that involves or permits multiple payments or transactions. Covered accounts also include any account for which there is reasonable foreseeable risk to the customer for identity theft. When we look at health care practices and covered accounts, two specifically come to mind. The first is the patient's financial account. This account contains patient demographic information, financial information and claims transactions. The second account includes the patient's health care record. In the downturn of the economy, patients are losing their jobs and health care benefits. This could result in some patients turning to fraudulent means to have access to care, as was the situation in the following case study.

Case Study

A patient presented to a Physician's office and provided a photo driver's license identification, his red, white and blue Medicare card and a secondary insurance card. The patient was examined by the Physician who ordered lab tests and imaging studies. Several weeks later, the office answered a phone call from a person who had received a bill from the Physician claiming he had never seen this Physician. The office, upon in-depth questioning of the person on the phone, later concluded that the person receiving the bill was ***not*** *the person who had received care. The person presenting to the office was, in fact, the brother of the person calling with the complaint. The person presenting to the office did* ***not*** *have health insurance coverage and was fraudulently using his brother's identity.*

After this discovery, the office was required to return the money to the insurance carriers and could not hold the brother with health insurance liable for the balance. They could hold the person receiving treatment responsible for the full balance on the account.

Additionally, the office had the obligation of notifying the laboratory and the imaging center of the identity theft.

Identify and Detect

The FTC's Red Flags Identity Theft Provention Policy requires health care practices to have a written policy in place to identify and detect changes, inconsistencies, complaints, or unusual practices, patterns or activities that would send up a "red flag" about the identity of the patient. For example, in the above case study, the practice recognized the identity theft from a complaint that medical services had not been rendered. Other examples might be unusual or frequent address changes, inconsistencies in the patient's name and the name on the insurance card or a form of payment that

does not match the patient's identity (i.e. a credit card in someone else's name).

Respond

The written policy must also include how you respond to any red flags that may occur. For example, in the case study above, it may be as simple as asking questions. It may be that you verify information by requesting additional forms of identification or that you check outside sources such as referring Physicians or hospitals that would have information on the patient.

Once you have established that the information is not correct and that the identity has been stolen, you ***must*** have the person reporting the theft sign a statement that the services were not received. The FTC has a sample affidavit that can be completed by the person claiming the identity theft. (See *Resources* section of this newsletter.)

In addition, if the person whose identity has been stolen is an established patient, you must give the patient a new account number and chart. The information obtained by the person who presented fraudulently must also be given a new account number and chart, labeled as "John Doe" or "unknown." Moreover, you may not hold the person whose identity was stolen responsible for the bill or for correcting fraudulent health care information. Finally, you have an obligation to report this information to other health care providers with whom you have exchanged information.

Written Policy

Your written policy should answer the following questions:

- What type of accounts does your practice offer?
  - Financial
  - Health record

- What methods do you use to open an account?
  - List your new patient registration forms and identifying information that you collect
  - List the method you use to set up new patients when the patient is first seen in the hospital

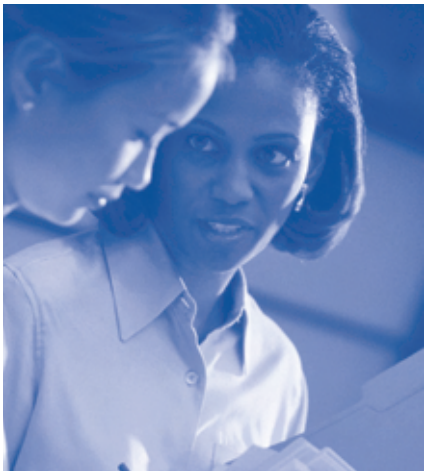
- What methods do you use to access each account?
  - List staff and how they access the accounts
    - Billing personnel post charges and payments
    - Health care staff enters medical information

- Has your office had any previous experience with identity theft?
  - If yes, describe the incident
  - If no, state "none at this time"

- What methods does your office use to **Identify and Detect** identity theft?
  - See *Identify and Detect* section of this newsletter

- How does your office **Respond** to suspected identity theft?
  - See *Response* section of this newsletter

- Perform a risk analysis to identify any gaps in identifying possible theft.
  - Ask yourself what types of activities your



office performs and if there are processes in place to capture and send an alert for possible theft

- Do you work with other service providers that may help you identify theft?
  - A service provider may be an outside billing company or collection agency.
  - Request a copy of their identity theft policy and keep a copy with your policy

Administration

Now that your written policy is complete, it must be signed by the owner(s) of the business. As with all parts of the identity theft program, it is meant to be scalable. If you have a large group of providers and a governing board, the board is required to sign the written policy. If your office consists of one Physician and one staff member, the Physician owner must sign the policy.

Each practice must designate an oversight officer. This person is responsible for implementing the policy, organizing staff training and having a written policy available at each location. The oversight officer is also required to write a yearly report to the business owner(s) regarding compliance with the program.

This yearly compliance report should evaluate how effective the policy has been over the past twelve months. The report should also address the following questions: 1) Have there been any incidences of identity theft and, if so, how were each of these incidences handled? 2) Have there been any changes in your current practice that would increase or decrease the risk of identity theft? For example, have you opened or closed any office locations? 3) Are you working with any new service providers such as e-prescribing companies or electronic health record vendors? 4) Do you have any recommendations for improving the identity theft program? Staff training and review of your written policy should be conducted each year.

The Red Flags Identity Theft Prevention Policy is a working policy and should not be created and forgotten. The FTC has already established civil monetary sanctions of $2,500 for each incidence of non-compliance. It is important that your patients know that you take identity theft seriously and that you are in compliance with these new regulations. Your patients may have questions about changes that you need to make in your office in order to comply. For example, you may ask your patients for a copy of their photo identification. In a pediatric practice, the office would collect identifying information on the adult bringing the child for treatment. Remember, this policy is an **internal** working document; it does not need to be signed by patients or sent to the FTC. However, the FTC does have authority to inspect the working policy and audit the yearly compliance report.

Resources

There are many resources for health care practices to help create and implement an identity theft prevention program:

- Federal Trade Commission *(www.ftc.gov)*
  "Fighting Fraud with the Red Flag Rules: A How-To Guide for Business"
  www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf

- American Medical Association *(www.ama-assn.org)*
  "AMA Identity Theft Prevention and Detection and Red Flags Rule Compliance Sample Policy"
  www.ama-assn.org/ama1/pub/upload/mm/368/red-flags-rule-policy.pdf

- American Hospital Association *(www.aha.org)*
  "Red Flags Identity Theft Prevention Program, Sample"
  www.aha.org/aha/content/2008/document/08redflagsoverview.doc

- MedChi, The Maryland State Medical Society (*www.medchi.org)*
  "MedChi Weekly Tips for Red Flags"
  www.medchi.org/lawandadvocacy/index.asp
  *requires a MedChi membership

So, whether you call it "a gut feeling," "a women's intuition" or the information just doesn't add up, it is time to raise the Red Flag. The identity theft prevention policy requires practices to ensure that the information they are receiving from the patient is accurate and belongs to the patient presenting for treatment. This policy will add integrity to Federal HIPAA Privacy and Security policies that require practices to protect a patient's health information when maintaining and disclosing protected information.

Doctors RX

Elizabeth A. Svoysky, J.D., *Editor*
Assistant Vice President - Risk Management

Dr. George S. Malouf, Jr., M.D., *Chair of the Board*
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

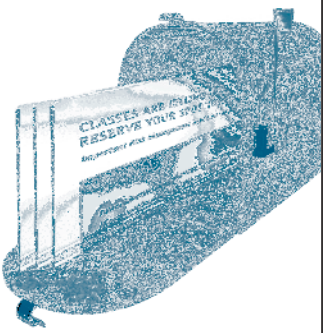
Numbers you should know!

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	ext. 163
Risk Management Seminar Info	ext. 215 or 225
Risk Management Questions	ext. 224
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	www.weinsuredocs.com

Risk Management Reminder #2 to be Mailed Soon

A second risk management seminar reminder will be mailed to all MEDICAL MUTUAL/Professionals Advocate Insureds in July. These reminder mailings are important, as they provide updated information on currently available courses and locations. The reminders also include any recently added courses that weren't available in the original seminar brochure or first reminder mailing.

If you haven't done so, there is still time to attend one of our informative and instructive risk management educational seminars. Please register today to ensure you get the topic, date and location of your choice. Don't miss out on this opportunity to build a stronger practice.



Publication of MEDICAL MUTUAL / Professionals Advocate®

DOCTORS Rx

Volume 17, No. 2 Special Edition 2009

MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate Insurance Company
Home Office: Box 8016, 225 International Circle
Hunt Valley, MD 21030 • 410-785-0050 • 800-492-0193

PRST STD
U.S. POSTAGE
PAID
PERMIT NO. 5415
BALTIMORE, MD