

# TPR Spotlight

www.totalpracticeresources.com

(303) 242-8901

## The Red Flag Rules & What It Means To You...

### What is Medical Identity Theft?

#### What you need to know:

Medical identity theft occurs when a person's name and other parts of their identity, possibly even insurance information are used without consent or are stolen. When this occurs, the victim's medical identity is used to obtain medical services or products. This, of course, generally results in wrongful entries and documentation in the victim's medical records which is potentially extremely dangerous.

Victims of medical identity theft may have incorrect diagnosis added to their records and may receive false treatment in medical centers, be prescribed incorrect medication by pharmacies, find that their medical benefits through insurance have been exhausted, etc. As it is so difficult to discover and correct this, many false entries in records are never even discovered!

#### What's Next with Medical Identity Theft?

Resources say that a roughly estimated quarter million to half million people have been victimized by Medical Identity Theft and this number continues to grow.

As medical records are transitioning from the traditional paper format to electronic records, this actually is likely to make it easier for Medical Identity Theft crimes to be committed and even more difficult for providers and patients to discover and correct these errors.

As we have many rights and abilities to correct our Financial Identity (credit cards, checking accounts, etc) and can monitor this regularly through credit bureaus and other resources, we do not have these same rights or

In fact, we cannot prevent our information from being forwarded to billing services, insurance companies, insurance clearinghouses, etc.

Many changes are underway and requirements for providers are being established.

Patients and providers ability to learn of medical data breaches has the potential to save lives, protect health, and prevent financial losses. Extensive studies are underway to determine how to detect and prevent Medical Identity Theft.

### **Are you affected by the Red Flag Rules?**

A health care provider comes under the Red Flag rule if the provider:

1) meets the definition of creditor under the Fair Credit Reporting Act (15 U.S.C. 1681a(r)(5)).

A Creditor is: any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. 15 U.S.C. §§ 1691a(e), 1681a(r)(5). 16 C.F.R. § 681.2(b)(4).

Creditors that offer or maintain covered accounts have obligations under the Red Flag regulations. A covered account is:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and  
(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. 16 C.F.R. § 681.2(b)(3).

*Basically, this means that if a health care provider extends*

*account that permits multiple payments, the provider is a creditor offering a covered account and is subject to the Red Flag rules.*

\*Resource: [www.worldprivacyforum.org](http://www.worldprivacyforum.org)

## **What are Providers Obligations Under the Red Flag Rules?**

If a health care provider falls under the Red Flag Rule as a creditor, the provider must develop and implement a written identity theft prevention program.

The rule requires a periodic evaluation to determine whether covered accounts are offered.

For those creditors required to have an Identity Theft Prevention Program, there are four required elements. The program must include reasonable policies and procedures to:

1. Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program
2. Detect Red Flags that have been incorporated into its program
3. Respond appropriately to any Red Flags that are detected
4. Update the program periodically to reflect changes in risks from identity theft to customers and to the safety and soundness of the creditor regarding identity theft.

There are also four elements to the administration of the Identity Theft Prevention Program. Each creditor required to have a program must:

1. Obtain approval of the initial written program from either its board of directors or an appropriate committee of the board of directors
2. Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the program
3. Train staff, as necessary, to effectively implement the program
4. Exercise appropriate and effective steps to implement and maintain these policies.

The following list of Red Flags is geared specifically to health care providers and is offered as a focused addition

- 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
- an Explanation of Benefits or other notice for health services never received.
- Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient.
- A complaint or question from a patient about the receipt of a collection notice from a bill collector.

- 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.
- A complaint or question from a patient about information added to a credit report by a health care provider or insurer.
- A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
- A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency. Health care providers subject to the rules need to go beyond the provisions in HIPAA to assist victims.

There needs to be uniform but appropriately flexible answers to these questions:

- \* What do we do when a patient claims fraud is in their files?
- \*What do we do when a patient says the bills are for services he/she did not receive?
- \* What do we do for patients and other impacted victims when we uncover a fraudulent operation?
- \* When we have a real case of medical identity theft, how can we work with patients to fix the records and limit future damages?
- \* What do we do when a provider has altered the patient records?
- \* How do we handle police reports and requests for investigation from victims?

Providers and other professionals in the health care sector need to begin patient and victim education regarding

education should focus on increasing:

- \*Awareness of the crime

- \*Awareness of the benefits of requesting a full copy of the health care files from all providers proactively

- \*Awareness of the need to guard insurance and Medicare/Medicaid card numbers as carefully as Social Security Numbers

- \*Awareness of the need to proactively request an annual listing of all benefits paid by insurers

- \*Awareness of the need to educate data breach and financial identity theft victims about the potential for medical identity theft variations of the crime.

- \*Patient education and training on how to handle their health and insurance records securely, and on increasing awareness of the need for laptops, desktops, and other devices used that contain sensitive health or financial information and the need for those things to have security features.

resource: [www.worldprivacyforum.org](http://www.worldprivacyforum.org)