



# TPR Spotlight

October, 2009

## In This Issue

Introduction

Implementing Red Flag Rules

HealthCare Payment Solutions

Dear Doctors,

As you may feel overwhelmed by constant changes in rules and requirements as well as your individual practice needs, this month's newsletter offers additional information and assistance to you for some of these hot topics.

Below, you will see additional information and resources to help better understand some of these changes as well as learn to maximize systems in your practice.

## Implementing the Red Flag Rules

The Red Flag Regulations apply to any company that provides goods or services without demanding payment up front.

Under the Red Flag Regulations, creditors must establish a comprehensive identity theft prevention program. The provider must be able to demonstrate that it has established reasonable policies and procedures to "detect, prevent and mitigate identity theft in connection with the opening of a Covered Account or any existing Covered Account. The program must be periodically updated to reflect changes in risks.

Before drafting the Program, a Provider may consider assembling a team to perform a risk assessment. The Risk Assessment Team (your entire staff) should review and determine risk in all of your office departments; patient check in/out, verification of medical coverage, safeguarding patient information, billing for services, etc. The Risk Assessment Team should review how a patient's identity is verified when opening a new patient account, what information is gathered, how that information is stored, and what steps could be taken to detect and prevent identity theft in connection with existing accounts.

Assembling a Risk Assessment Team is not a regulatory requirement. If one employee is well-versed in all aspects of a Provider's operation, that employee could perform the risk assessment with the involvement of the owner(s)/doctor(s).

Next, the Risk Assessment Team should take the following steps to develop the identify theft Program:

**Identify Covered Accounts** -- The Risk Assessment Team should identify and list the Covered Accounts. The Team should think of every way a would-be identity thief could take advantage of the Provider's relationship with its residents or patients.

**Identify Red Flags** -- A Provider's written Program should list identity theft Red Flags. A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. For example, the following are common Red Flags: presentation of documents that look to be forged, altered, or fake; a suspicious address change; and a resident demanding services or access to health records with unusual urgency or frequency. Of course, any warning from law enforcement or a consumer reporting agency that a resident may be an imposter should be taken seriously. A Provider should include additional Red Flags from its own experiences with identity theft, as well as the applicable suggested Red Flags contained in the regulations.

**Assess the Risk Level** -- When the Risk Assessment Team develops a list of the hypothetical ways that identity theft or medical identity theft of patients could occur, the Team should then consider the real-life likelihood of each particular risk coming to pass. Some routes to identity theft are more likely than others.

**Determine the Appropriate Response** -- Taking into consideration the relevant Red Flags the Provider has identified and the potential risk level for identity theft, including medical identity theft, the Team must then determine the appropriate response to those Red Flags. Example: If the Red Flag is an address discrepancy, the response may be to ask for

additional identification.

Document Results of the Risk Assessment -- For compliance purposes, it is important for the Provider to document the results of the risk assessment. A well-documented and thought-out risk assessment process will help satisfy regulators and may potentially save money by avoiding security breaches and compliance issues.

Prepare the Identity Theft Program -- The next step is to incorporate the findings from the risk assessment and prepare the written Program. Although some of the policies and procedures may already be documented in existing Information Security, HIPAA or other policies, it is a best practice to have a separate document that either sets out separately the Program, or points to the specific places in existing policies that comply with the Red Flag Regulations. Required Approval -- A designated employee or administrator must review and approve as well as help develop, implement and oversee the Program. Be certain to assign responsibility for the Program's implementation and compliance, reviewing reports prepared by staff, training staff as necessary to effectively implement the Program, overseeing service provider arrangements as appropriate, and approving material changes to the Program.

Report Annually -- Provider or employee who has the designated responsibility of development, implementation, and administration of the Program must report to the Administrator at least annually regarding compliance with the Red Flag Regulations. The annual report should address such items as the policies and procedures of the Program, service provider arrangements, significant incidents of identity theft and the responses taken to same, as well as recommendations for material changes to the Program.

Assign Responsibility -- As with any 'blue prints', your written program for identity theft protection is only worthwhile if someone actually implements it. The Administrator may delegate responsibilities but ultimately is responsible for overseeing the Program. For example, the Administrator may delegate responsibility for training employees to a designated person, and oversight of service provider arrangements to another.

Train Staff -- All staff with access to Covered Accounts must be trained as necessary regarding the policies and procedures that are applicable to their job function. This would include training upon hiring, follow-up training as needed, and training on new policies or procedures when the Program is updated.

Review Service Provider Arrangements -- If a Provider engages service providers to perform services in connection with Covered Accounts (e.g., a billing agent or management company), the Provider must take steps to ensure that the service provider has reasonable policies in place to detect, prevent, and mitigate the risk of identity theft. This can be accomplished by requiring the provider via contract to have policies and procedures to detect relevant Red Flags that may arise in connection with the provision of services, and either to report the Red Flags to the Provider or take appropriate steps to prevent, detect and mitigate identity theft by setting up its own Program.

All Healthcare facilities should promptly take steps to establish their written identity theft program.

## HealthCare Payment Solutions

Are you looking for a better avenue to offer service to patients and collect for your services rendered? Total Practice Resources recommends HealthCare Payment Solutions to you as a solution to this obstacle that many offices are having.

HealthCare Payment solutions has many beneficial features that you may find will aid in your increasing of efficiencies with collections as well as increasing your profits.

HealthCare Payment Solutions uses auto-debit billing (similar to that in fitness centers), and spread payments out over time from patients' bank accounts in an amount that is pre-determined and agreed upon. Following this, the payments are instantly deposited into the practice bank accounts.

You can use this system to collect deductibles, non-insurance charges, etc.

As a third party company is now taking care of payment issues, this will free up time and efforts in your practice and allow you to increase time spent and productivity in other areas of your practice.

For more information, visit [www.healthcarepaymentsolutions.com](http://www.healthcarepaymentsolutions.com) or call 866-657-2009 and ask for Darius Martino. You may also reach Darius directly at (727) 902-7311. A special negotiated sign up discount is in place for all referrals from Total Practice Resources. Should you take advantage of the benefits of HealthCare Payment Solutions, be sure to let them know you have been referred by Total Practice Resources to receive this discount on your sign up.

## Webinars

New webinars are available now through Total Practice Resources. We are also offering FREE webinars with further education on insurance claim submissions and clearinghouses as well as how to better utilize Nutri-West Nutrition in your practice. Be sure that you take advantage of these webinars offered as they are full of invaluable information for your practice growth and development.

For more information on the Total Practice Resources programs or to speak with one of our consultants, please visit us online at [www.totalpracticeresources.com](http://www.totalpracticeresources.com) or call us at (303) 242-8901. To reach Brandy directly by e-mail, submit questions or requests to [brandy\\_tpr@yahoo.com](mailto:brandy_tpr@yahoo.com).

Thank you for viewing this addition of the TPR Spotlight.

### [Forward email](#)

✉ **SafeUnsubscribe®**

This email was sent to [brandy\\_tpr@yahoo.com](mailto:brandy_tpr@yahoo.com) by [brandy\\_tpr@yahoo.com](mailto:brandy_tpr@yahoo.com).

[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by



Total Practice Resources | 9142 Lodestar Lane #203 | Parker | CO | 80134