

Red Flags Rules

The growing threat of identity theft has made its mark on the health care world. January 1, 2008 marked the inception of the “Red Flags Rule,” mandated by the Federal Trade Commission (FTC). The rule, which will become mandatory on June 1, 2010, will force creditors to take steps towards the prevention of identity theft.

Below is the information and guidance prepared for the Federal Trade Commission on Red Flags Rules for Health Care providers. This document offers a detailed overview of the rule and guidelines on the requirements for health care organizations. This is followed by a sample policy for home health agencies, hospices, DME suppliers, and private duty agencies to use to implement the Red Flags Rule consistent with the FTC guidance.

What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft

As many as nine million Americans have their identities stolen each year. The crime takes many forms. But when identity theft involves health care, the consequences can be particularly severe.

Medical identity theft happens when a person seeks health care using someone else’s name or insurance information. A survey conducted by the Federal Trade Commission (FTC) found that close to 5% of identity theft victims have experienced some form of medical identity theft. Victims may find their benefits exhausted or face potentially life-threatening consequences due to inaccuracies in their medical records. The cost to health care providers — left with unpaid bills racked up by scam artists — can be staggering, too.

The Red Flags Rule, a law the FTC will begin to enforce on June 1, 2010, requires certain businesses and organizations — including many doctors’ offices, hospitals, and other health care providers — to develop a written program to spot the warning signs — or “Red Flags” — of identity theft. Is your practice covered by the Red Flags Rule? If so, have you developed your Identity Theft Prevention Program to detect, prevent, and minimize the damage that could result from identity theft?

Who Must Comply

Every health care organization and practice must review its billing and payment procedures to determine if it’s covered by the Red Flags Rule. Whether the law applies to you isn’t based on your status as a health care provider, but rather on whether your activities fall within the law’s definition of two key terms: “creditor” and “covered account.”

Health care providers may be subject to the Rule if they are “creditors.” Although you may not think of your practice as a “creditor” in the traditional sense of a bank or mortgage company, the law defines “creditor” to include any entity that regularly defers payments for goods or services or arranges for the extension of credit. For example, you are a creditor if you regularly bill individuals after the completion of services, including for the remainder of medical fees not reimbursed by insurance. Similarly, health care providers who regularly allow individuals to set up payment plans after services have been rendered are creditors under the Rule. Health care providers are also considered creditors if they help individuals

get credit from other sources — for example, if they distribute and process applications for credit accounts tailored to the health care industry.

On the other hand, health care providers who require payment before or at the time of service are not creditors under the Red Flags Rule. In addition, if you accept only direct payment from Medicaid or similar programs where the individual has no responsibility for the fees, you are not a creditor. Simply accepting credit cards as a form of payment at the time of service does not make you a creditor under the Rule.

The second key term — “covered account” — is defined as a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft. The accounts you open and maintain for your individuals are generally “covered accounts” under the law. If your organization or practice is a “creditor” with “covered accounts,” you must develop a written Identity Theft Prevention Program to identify and address the Red Flags that could indicate identity theft in those accounts.

More About Creditors and Covered Accounts

Creditors: According to the FTC, the definition of “creditor” is broad and includes businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later. Utility companies, health care providers, and telecommunications companies are among the entities that may fall within this definition, depending on how and when they collect payment for their services.

The Rule also defines a “creditor” as one who regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions. Examples include finance companies, mortgage brokers, real estate agents, automobile dealers, and retailers that offer financing or help consumers get financing from others, say, by processing credit applications. In addition, the definition includes anyone who regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit – for example, a third-party debt collector who regularly renegotiates the terms of a debt. If you regularly extend credit to other businesses, you also are covered under this definition.

Covered Accounts Once you’ve concluded that your business or organization is a financial institution or creditor, you must determine if you have any “covered accounts,” as the Red Flags Rule defines that term. To make that determination, you’ll need to look at both existing accounts and new ones. Two categories of accounts are covered. The first kind is a consumer account you offer your customers that’s primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Examples are credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

The second kind of “covered account” is “any other account that a 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.” Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to permit multiple payments or transactions – they always are “covered accounts” under the

Rule – other types of accounts are “covered accounts” only if the risk of identity theft is reasonably foreseeable.

Determining if Accounts are Covered: In determining if accounts are covered under the second category, consider how they’re opened and accessed. For example, there may be a reasonably foreseeable risk of identity theft in connection with business accounts that can be accessed remotely – such as through the Internet or by telephone. Your risk analysis must consider any actual incidents of identity theft involving accounts like these.

Applicability to Home Health Agencies, Hospices, and DME Suppliers, and Private Duty Agencies

Home health agencies, hospices, DME suppliers and home care aide providers need to understand that the Red Flags Rule has only limited effect upon health care providers. The rule is limited to covered accounts in which individuals will be paying all or part of the cost of health care services previously furnished to them. The intent of Red Flags rules is to protect individuals from being charged for debts incurred by another person who seeks health care using that individual’s name or insurance information. When Medicare, Medicaid and/or a third party payer will pay all of the costs of the services furnished, and no costs will be billed to the individual, then the Red Flags Rule does not apply. If all copays or deductibles, and in the case of private pay—payment in full-- are collected from the individual prior to the furnishing of services, and the individual will have no obligation for further payment for the services, then the Red Flags rule does not apply.

For accounts in which the individual will be making payment(s) after services are furnished, the Red Flags rule applies. The Rule protects the individual from theft of the individual’s identify tied to the account in which the individual is making payments.

Many home care providers and suppliers, however, have a different concern regarding identity theft—medical identity theft. Providers and suppliers may be concerned that an individual will claim to have Medicare coverage, but be fraudulently assuming a Medicare beneficiary’s identity to obtain care and supplies. In these cases, the agency may want to establish policies requiring all individuals produce insurance cards and photo identification in order to protect themselves against payment denials, as well as protect individuals whose identities have been stolen.

Red Flags Rule Guidance

SPOTTING RED FLAGS

The Red Flags Rule gives health care providers flexibility to implement a program that best suits the operation of their organization or practice, as long as it conforms to the Rule's requirements. Your office may already have a fraud prevention or security program in place that you can use as a starting point.

If you're covered by the Rule, your program must:

1. Identify the kinds of Red Flags that are relevant to your practice;
2. Explain your process for detecting them;
3. Describe how you'll respond to Red Flags to prevent and mitigate identity theft; and
4. Spell out how you'll keep your program current.

What Red Flags signal identity theft? There's no standard checklist. Supplement A to the Red Flags Rule — available at [ftc.gov/redFlagsrule](https://www.ftc.gov/redFlagsrule) — sets out some examples, but here are a few warning signs that may be relevant to health care providers:

Suspicious documents. Has a new individual given you identification documents that look altered or forged? Is the photograph or physical description on the ID inconsistent with what the individual looks like? Did the individual give you other documentation inconsistent with what he or she has told you — for example, an inconsistent date of birth or a chronic medical condition not mentioned elsewhere? Under the Red Flags Rule, you may need to ask for additional information from that individual.

Suspicious personally identifying information. If an individual gives you information that doesn't match what you've learned from other sources, it may be a Red Flag of identity theft. For example, if the individual gives you a home address, birth date, or Social Security number that doesn't match information on file or from the insurer, fraud could be afoot.

Suspicious activities. Is mail returned repeatedly as undeliverable, even though the individual still shows up for appointments? Does an individual complain about receiving a bill for a service that he or she didn't get? Is there an inconsistency between a physical examination or medical history reported by the individual and the treatment records?

These questionable activities may be Red Flags of identity theft.

Notices from victims of identity theft, law enforcement authorities, insurers, or others suggesting possible identity theft. Have you received word about identity theft from another source? Cooperation is key. Heed warnings from others that identity theft may be ongoing.

SETTING UP YOUR IDENTITY THEFT PREVENTION PROGRAM

Once you've identified the Red Flags that are relevant to your practice, your program should include the procedures you've put in place to detect them in your day-to-day operations. Your program also should describe how you plan to prevent and mitigate identity theft. How will you respond when you spot the Red Flags of identity theft? For example, if the individual provides a photo ID that appears forged or altered, will you request additional documentation? If you're notified that an identity thief has run up medical bills using another person's information, how will you ensure that the medical records are not

commingled and that the debt is not charged to the victim? Of course, your response will vary depending on the circumstances and the need to accommodate other legal and ethical obligations — for example, laws and professional responsibilities regarding the provision of routine medical and emergency care services. Finally, your program must consider how you'll keep it current to address new risks and trends. No matter how good your program looks on paper, the true test is how it works. According to the Red Flags Rule, your program must be approved by your Board of Directors, or if your organization or practice doesn't have a Board, by a senior employee. The Board or senior employee may oversee the administration of the program, including approving any important changes, or designate a senior employee to take on these duties. Your program should include information about training your staff and provide a way for you to monitor the work of your service providers — for example, those who manage your individual billing or debt collection operations. The key is to make sure that all members of your staff are familiar with the Rule and your new compliance procedures.

WHAT'S AT STAKE?

Although there are no criminal penalties for failing to comply with the Rule, violators may be subject to financial penalties. But even more important, compliance with the Red Flags Rule assures your individuals that you're doing your part to fight identity theft.

Looking for more information about the Red Flags Rule? The FTC has published [Fighting Fraud with the Red Flags Rule: A How-To Guide for Business](#), a plain-language handbook on developing an Identity Theft Prevention Program. For a free copy of the Guide and for more information about compliance, visit ftc.gov/redFlagsrule.

In addition, the FTC has released a fill-in-the-blank form for businesses and organizations at low risk for identity theft. The online form offers step-by-step instructions for creating your own written Identity Theft Prevention Program. You can fill it out online and print it. The do-it-yourself form is available at ftc.gov/redFlagsrule.

Complying with the Red Flags Rule: A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program to detect the warning signs – or “Red Flags” – of identity theft in their day-to-day operations. By focusing on Red Flags now, you’ll be better able to spot an imposter using someone else’s identity to get products or services from you. As a practical matter, the Rule applies to you if you provide products or services and bill customers later. To find out if the Red Flags Rule applies to your business, read [Fighting Fraud with the Red Flags Rule: A How-To Guide for Business](#), a booklet published by the Federal Trade Commission (FTC).

The FTC, the federal agency that enforces a number of consumer protection laws, has designed this compliance template to help businesses and organizations at low risk for identity theft design their own Identity Theft Prevention Program. It has two parts: Part A to help you determine whether your business or organization is at low risk, and Part B to help you design your written Identity Theft Prevention Program if your business is in the low risk category.

How can you tell if your business is at low risk for identity theft? Conduct an assessment. Although you have to consider the unique characteristics of your business, here are some factors to help you decide your risk level.

Do you know your clients personally? Perhaps you’re a doctor or a lawyer on Main Street and are familiar with everyone who walks into your office. It’s unlikely that an identity thief can defraud you by impersonating someone you already know. That would place your business at low risk for identity theft.

Do you usually provide your services at your customers’ homes? To avoid getting caught, identity thieves tend to move around a lot. They generally don’t want people to know where they live. If you regularly provide services at your customers’ homes, your business may be at low risk for identity theft.

Have you ever experienced an incident of identity theft? You’ve been in business for some time now, and no one has complained that someone stole his identity and used it to get products or services at your business. That might suggest your business is at low risk for identity theft.

Do It Yourself Prevention Program

PART A:

Is your business or organization at low risk for identity theft?

How can you tell if your business is at low risk for identity theft? Conduct an assessment. Although you have to consider the unique characteristics of your business, here are some factors to help you decide your risk level.

Do you know your clients personally?

Perhaps you're a doctor or a lawyer on Main Street and are familiar with everyone who walks into your office. It's unlikely that an identity thief can defraud you by impersonating someone you already know. That would place your business at low risk for identity theft.

Do you usually provide your services at your customers' homes?

To avoid getting caught, identity thieves tend to move around a lot. They generally don't want people to know where they live. If you regularly provide services at your customers' homes, your business may be at low risk for identity theft.

Have you ever experienced an incident of identity theft?

You've been in business for some time now, and no one has complained that someone stole his identity and used it to get products or services at your business. That might suggest your business is at low risk for identity theft.

Are you in a business where identity theft is uncommon?

If there are no reports in the news and no talk among people in your line of work about identity theft, your industry may not now be the target of identity thieves, and your organization may be at low risk for identity theft.

Part B

Designing an identify theft program for businesses that are at low risk.
Here are the reasons we are at low risk for identity theft:

Designing a program involves four basic steps:

STEP 1: Identifying relevant Red Flags

STEP 2: Detecting Red Flags

STEP 3: Responding to Red Flags

STEP 4: Administering your Program

My Identity Theft Prevention Program

Step 1.

The first step is to identify the relevant Red Flags you might come across that signal that people trying to get products or services from you aren't who they claim to be. Read the FTC's free booklet [Fighting Fraud with the Red Flags Rule: A How-To Guide for Business](#) (pages 19-21) for examples. For instance, if you check photo IDs, a classic Red Flags of identity theft is an inconsistency between the person's appearance and the information on the photo ID. If you know all your customers personally, it's probably not necessary to ask for a photo ID, and this Red Flags wouldn't be appropriate. Sometimes, the only Red Flags

may be a notice from another source that an identity theft has occurred. Since that Red Flags applies to everyone, it's included here.

- Here are the Red Flags we have identified:
 - 1.
 - 2.
 - 3.Etc.

Step 2.

The second step is to explain how your business or organization will detect the Red Flags you've identified. For example, perhaps in Step 1 you identified false IDs as a Red Flags. To detect a false ID, you might consider training your staff to look carefully at the ID to see if the person's appearance is consistent. What if somebody notifies you that an account has been opened or used fraudulently? To make sure those notices don't fall through the cracks, you may decide to require employees to log that kind of notice in a central place or to tell a staff member responsible for responding to Red Flags.

- Here's how we'll detect the Red Flags we have identified:
 - 1.
 - 2.
 - 3.Etc.

Step 3.

The third step is to decide how you'll respond to any Red Flags that materialize. For example, say you've identified the risk of false IDs as a warning sign of identity theft, and you've noted that you will train your staff to look for inconsistencies in identification. Your employee has checked the photo ID and detected an inconsistency. What's the next step? Perhaps it's asking for another form of identification – or maybe not providing any products or services until the inconsistency has been resolved. Or imagine you're trying to collect on an unpaid bill, and the person you contact tells you his identity was stolen and he didn't run up that bill. Although it will depend on the circumstances, consider how you might respond. For example, you could ask for proof that an identity theft claim has been filed.

- Here's how we'll respond to the Red Flags we have identified:
 - 1.
 - 2.
 - 3.Etc.

Step 4.

The last step is documenting how you'll administer your Program. Here's what's involved: Get the approval of your Board of Directors, a committee of your Board, or a senior manager, designate a senior employee to administer your Program, describe how you'll train your staff. • List the categories of employees who will be trained to detect Red Flags – for example, your reception staff or the people who handle your accounts

receivable – and how they’ll get that training – say, during an orientation for new employees or an annual update.

- Here are the categories of employees we’ll train and how we’ll provide training
 - 1.
 - 2.
 - 3.Etc.

Describe how you’ll supervise your service providers. Do you use service providers who might detect any of the Red Flags you’ve identified? For example, do you hire a company to handle your invoicing or use a collection agency to collect overdue bills? Talk to them to see that they’re following your Program or have their own that complies with the Red Flags Rule. Determine if service providers are used in connection with accounts covered by Red Flags Rule.

We don’t use service providers in connection with accounts covered by the Red Flags Rule.
We use service providers in connection with accounts covered by the Red Flags Rule.

- Here are the service providers we’ll contact about complying with the Red Flags Rule:
 - 1.
 - 2.
 - 3.Etc.

Describe how you’ll update your Program. • Identity theft risks can change fast, so it’s important to reassess your Program periodically. If your business experiences identity theft, if any factors change that contributed to your original assessment of low risk, or if you change your business model with respect to your accounts or your corporate structure, you will need to re-evaluate and modify your Program.

- Here is how we will keep our program current:
 - 1.
 - 2.
 - 3.Etc.

SAMPLE

RED FLAGS IDENTITY THEFT PREVENTION PROGRAM

[DATE]

[items to be modified are in italics and brackets]

The Board of [Directors/Trustees] of [Home Health, Hospice, or Private Duty Agency or DME supplier] (“Agency”) approved this Identity Theft Prevention Program (“Program”) at a duly held meeting on _____, 2009. The Program was developed in order to comply with the Federal Trade Commission’s Identity Theft Prevention Red Flags Rule (16 CFR § 681.2). This Program has been created in consultation with [INSERT RELEVANT GROUPS AND DIVISIONS], [Individual Billing, IT, Medical Records, and the Legal Department], after conducting an assessment of risk of Identity Theft associated with certain Covered Accounts (as defined below) offered by Agency.

I. Definitions

For purposes of the Program, the following terms are defined as:

“Covered Account” means a consumer account that allows multiple payments by individual or any other account with a foreseeable risk of identity theft. As of _____, Agency has identified as Covered Accounts all individual accounts in which Agency has not received payment in full from the individual at the time the service is rendered, and in which Agency expects all or part of the outstanding payment to be made by the individual. “Covered account” does not include accounts for which all payments will be made by Medicare, Medicaid and/or a third party payer.

“Identity Theft” means fraud attempted or committed using the identifying information of another person without authority;

“Red Flags” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

II. Program Purposes

The purposes of the Program are to:

- 1) Identify the relevant Red Flags based on the risk factors associated with the Agency’s _____ covered accounts;
- 2) Institute policies and procedures for detecting Red Flags;
- 3) Identify steps the institution will take to prevent and mitigate Identity Theft; and
- 4) Create a system for regular updates and administrative oversight to the Program.

III. Identification of Red Flags

The Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A) identifies the Red Flags that would be most relevant to Agency. The Red Flags generally fall within one of the following four general types of Red Flags:

- 1) Suspicious Documents;
- 2) Suspicious Personal Identifying Information;
- 3) Suspicious or Unusual Use of Covered Account; and
- 4) Alerts from Others (e.g. customer, Identity Theft victim, or law enforcement)

IV. Detection of Red Flags

In order to facilitate detection of the Red Flags identified in Appendix A, [appropriate Agency staff] will take the following steps to obtain and verify the identity of the person.

- A. New Individuals re: Covered Accounts
 - 1) Require identifying information (e.g., full name, date of birth, address, photo identification, government issued ID, insurance card, etc.)
 - 2) When available, verify information with insurance company's information
- B. Existing Covered Accounts
 - 1) Investigate complaints
 - 2) Verify Take further action, as needed, per Appendix A

V. Preventing and Mitigating Identity Theft

In order to prevent and mitigate the effects of Identity Theft, staff will follow the appropriate steps identified in the attached Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A).

VI. Program Administration

The [insert title of responsible individual or committee] is responsible for developing, implementing, administering and updating the Program. [TITLE] will be responsible for developing a training program for staff identified by [TITLE] as responsible for or having a role in implementing the Program. This Program will be coordinated with the Policies and Procedures we maintain for individual privacy under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

VII. Service Provider Arrangements

Agency will require, by contract, that service providers that perform activities in connection with Covered Accounts have policies and procedures in place designed to detect, prevent and mitigate the risk of Identity Theft with regard to the Covered Accounts.

VII. Updating of Program

The [INSERT RESPONSIBLE PERSON OR GROUP] will periodically review the effectiveness of the Program and update the Program to reflect the addition or removal of Covered Accounts, and changes in risks to individuals/covered account holders from Identity Theft.

Appendix A

Relevant Identity Theft Red Flags Mitigation and Resolution Procedures for Covered Accounts

IDENTITY THEFT RED FLAGS	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAGS [ONLY SUGGESTIONS]
Documents provided for identification appear to have been altered or forged, or are not consistent with what the individual looks like or information furnished by the individual.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Notify law enforcement if appropriate.
Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the insurance company, including home address, birth date or Social Security number.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Notify law enforcement if appropriate.
Individual has an insurance number but never produces an insurance card or other physical documentation of insurance.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	<p>Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary.</p> <p>If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with individual.</p> <p>If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential</p>

		fraudulent activity. Notify law enforcement if appropriate.
Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the individual (e.g., inconsistent blood type).	Investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: blood type, age, race, and other physical descriptions may be evidence of medical identity theft.	Depending on the inconsistency and review of previous file, either delay, do not open a new covered account, or terminate credit. ¹ If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity. If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with individual.
Complaint/inquiry from an individual based on receipt of: -a bill for another individual -a bill for a product or service that the individual denies receiving -a bill from a health care provider that the individual never patronized - a notice of insurance benefits (or Explanation of Benefits) for health services never received.	Investigate complaint, interview individuals as appropriate	Terminate credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity. Notify law enforcement if appropriate. If the results of the investigation do not indicate fraud, re-verify all

¹ Terminate consistent with state law regarding abandonment and your policy regarding same giving appropriate notice as required.

		contact and identifying information with individual.
Complaint/inquiry from an individual about information added to a credit report by a health care provider or insurer	Investigate complaint, interview individuals as appropriate	<p>Terminate credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity.</p> <p>Notify law enforcement if appropriate.</p> <p>If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with individual.</p>
Complaint or question from an individual about the receipt of a collection notice from a bill collector.	Investigate complaint, interview individuals as appropriate	<p>Terminate credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity.</p> <p>Notify law enforcement if appropriate.</p> <p>If the results of the investigation do not</p>

		indicate fraud, re-verify all contact and identifying information with individual.
Individual or insurance company report that coverage for agency services is denied because insurance benefits have been depleted or maximums reached, although the individual denies using that level of services previously.	Investigate complaint, interview individuals as appropriate	<p>Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. Terminate treatment/²credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity.</p> <p>Notify law enforcement if appropriate.</p> <p>If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with individual.</p>
Agency is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the agency has opened a fraudulent account for a	Investigation to determine if billing was made fraudulently.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as

² Terminate consistent with state law regarding abandonment and your policy regarding same giving appropriate notice as required.

<p>person engaged in identity theft.</p>		<p>necessary. Terminate treatment/³credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity.</p> <p>Notify law enforcement if appropriate.</p> <p>If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with individual.</p>
<p>Personal identifying information provided by the individual is associated with known fraudulent activity as indicated by internal or third-party sources used by Agency. For example:</p> <ul style="list-style-type: none"> - The address on an application is the same as the address provided on a fraudulent application; or - The phone number on an application is the same as the number provided on a fraudulent application. 	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Terminate credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>If the results of the investigation indicate fraud, place a Red Flags alert in the Medical Chart warning of potential fraudulent activity.</p> <p>Notify law enforcement if appropriate.</p> <p>If the results of the investigation do not</p>

³ Terminate consistent with state law regarding abandonment and your policy regarding same giving appropriate notice as required.

		indicate fraud, re-verify all contact and identifying information with individual.
--	--	--