

**VAN BUREN COMMUNITY MENTAL HEALTH AUTHORITY
POLICIES & PROCEDURES**

Title: Identity Theft Prevention Program
Originated: 10/22/09

Number: I.13
Approved By: Executive Team

DIRECTIVE:

The Program was developed for the purposes of complying with the Federal Trade Commission's ("FTC") Identity Theft Prevention Red Flags Rule (16 C.F.R. § 681.2). This Program was created after conducting an assessment of risk of identity theft associated with Covered Accounts offered Van Buren Community Mental Health Authority (hereinafter referred to as VBCMHA). Based on the guidance issued by the FTC, VBCMHA has determined that based on the nature of its business, previous history, and minimal amount of potential covered accounts, it is at low risk for identity theft as contemplated by the regulations.

DEFINITIONS: For purposes of this program document, the following terms are defined as noted below:

1. Covered Account is defined to mean (i) any account VBCMHA offers or maintains for services rendered to a customer, which involves multiple payments or transactions, including one or more deferred payments; and (ii) any other account VBCMHA identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of the organization from Identity Theft. As of October 1, 2009, VBCMHA has identified the following as a Covered Account:

The person is registered to receive services and seeks services and will be permitted to make payments to VBCMHA over time via a payment plan.

2. Identity Theft is defined to mean fraud committed using the identifying information of another person.
3. Red Flag is defined to mean a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

PROCEDURES:

Overview

According to the applicable regulations, the Program must include "reasonable" policies and procedures designed to:

- Identify relevant Red Flags;
- Detect Red Flags;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Create a system for regular updates and administrative oversight of the Program.

Administrative Responsibility, Oversight and Coordination With Outside Service Providers

The Identity Theft Compliance Officer (VBCMHA's Compliance Officer) is responsible for implementing, administering and updating this Program.

As part of the Officer's duties in administering the Program, the Officer will be responsible for training all applicable staff on this Program (this includes maintaining documentation of the training).

Identification, Detection and Mitigation Procedures

According to the regulations, in developing identity theft policies and procedures, each provider is required to consider the applicable guidelines set forth in Appendix A of the regulations.

Some of the issues in the guidelines applicable to a health care provider would include considering categories of identity theft red flags such as:

- Presentation of suspicious documents by the customer in connection with obtaining and paying for services (e.g., documents provided for identification in connection with obtaining services that appear to have been altered or forged or the picture identification is not consistent with the appearance of the customer who is presenting for services);
- Presentation of incomplete information by the customer in connection with demographic and payment information;
- Presentation of suspicious identifying information by the customer or inconsistent identifying information of the customer (e.g., suspicious change of address);
- Notice from a victim of identity theft or others that a person has engaged in identity theft or opened a fraudulent account.

Given the operational nature of VBCMHA and the nature of the delivery of services, the identity theft red flag rules will generally be applicable to VBCMHA at the time a customer presents identifying information in connection with obtaining services for which payment may be made over time to VBCMHA. Moreover, identity theft issues may also arise in the billing and collection process in connection with services rendered by VBCMHA. Accordingly, VBCMHA has adopted the Identity Theft Protocols and Procedures set forth in the attached **Exhibit A**.

In order to facilitate detection of identity theft red flags, appropriate staff will take the following steps to obtain and verify the identity of the person seeking services.

1. With Regard to New Customers:

- (1) Require complete identifying information of customers as part of the admission process (e.g., full name, date of birth, address, government-issued identification, insurance card, etc.). Staff should obtain and maintain copies of the customer's identification cards presented.
- (2) When available, verify information with the applicable insurance company of customer.

2. Existing Customers With Payment Plans:

- (1) Verify validity of requests for changes of billing address.

- (2) Verify identification of person before giving out any personal information and follow HIPAA privacy policies regarding same.

In order to prevent and mitigate the effects of identity theft, staff are required to follow the appropriate steps identified in the attached Identity Theft Protocols and Procedures set forth in Exhibit A to address issues. When an issue does arise, staff are required to immediately notify the compliance officer for investigation.

EXHIBIT A

IDENTITY THEFT RED FLAGS PROTOCOLS AND PROCEDURES

POTENTIAL RED FLAGS	PREVENTION/MITIGATION	RESOLUTION
Identification documents presented by customer appear to have been altered in some manner.	Require customer to provide additional information to verify identity prior to completing the admission or billing process.	Require the customer to provide additional documentation to resolve the identified discrepancy so that the admission and billing process can be continued.
Identifying information provided by the customer is inconsistent or contains irregularities.	Require customer to provide additional information to verify identity prior to completing the admission or billing process.	Require the customer to provide additional documentation to resolve the identified discrepancy so that the admission and billing process can be continued.
The SSN provided by the customer is the same as that submitted by another customer.	Require customer to provide additional information to verify identity prior to completing the admission or billing process.	Require the customer to provide additional documentation to resolve the identified discrepancy so that the admission and billing process can be continued.
Customer fails to produce insurance card or other documentation verifying insurance number.	Require customer to provide additional information to verify identity prior to completing the admission or billing process.	Require the customer to provide additional documentation to resolve the identified discrepancy so that the admission and billing process can be continued.
<p>Receipt of a complaint from a person that raises potential identity theft issues. For example, the person complains to VBCMHA based on receiving:</p> <ul style="list-style-type: none"> • a bill for another individual • a bill for a service or procedure that the person alleges that they did not receive from VBCMHA • Explanation of Benefits for services never received • other similar examples 	Investigate complaint, interview individuals as appropriate. Coordinate with outside service providers, as applicable. Involve legal counsel in investigation, as appropriate.	<p>Place the billing and collection process on hold until completion of the investigation.</p> <p>Permanently cease billing and collection efforts in the event that it has been determined that identity theft has occurred or that it is likely to have occurred. In such cases, promptly coordinate with the billing service or office (as applicable) and/or collection agency as applicable.</p> <p>Notify law enforcement as appropriate.</p>

POTENTIAL RED FLAGS	PREVENTION/MITIGATION	RESOLUTION
		<p>Address appropriate manner in which to handle any medical record issues that may have resulted from the identity theft (e.g., customer was not the person they claimed- a notation of the identity theft may need to be added to the record etc.)</p> <p>If the investigation does not reveal a problem, re-verify customer identifying information and correct any errors, as appropriate.</p>
<p>Notification from the billing office that a potential identity theft situation has occurred.</p>	<p>Work with the billing office to investigate the complaint, interview individuals as appropriate. Consult legal counsel as applicable.</p>	<p>Place the billing and collection process on hold until completion of the investigation.</p> <p>Permanently cease billing and collection efforts in the event that it has been determined that identity theft has occurred or that it is likely to have occurred. In such cases, promptly coordinate with the billing office and/or collection agency as applicable.</p> <p>Notify law enforcement as appropriate.</p> <p>Address appropriate manner in which to handle any medical record issues that may have resulted from the identity theft (e.g., customer was not the person they claimed- a notation of the identity theft may need to be added to the record etc.)</p> <p>If the investigation does not reveal a problem, re-verify customer identifying information and correct any errors, as appropriate.</p>

POTENTIAL RED FLAGS	PREVENTION/MITIGATION	RESOLUTION
<p>VBCMHA is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that an identity theft issue has occurred.</p>	<p>Investigate to determine if a billing was made to a person or insurance company based on the unknowing receipt of false information. Consult legal counsel as appropriate.</p>	<p>If identity theft did occur, stop and correct any billing or collection process. Contact insurance company as necessary.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate an issue, all contact and identifying information is re-verified with patient.</p>