

## ATTACHMENT 2

### **Identity Theft Prevention Program Policy & Procedures**

**Effective Date:** May 1, 2009

#### **I. PURPOSE**

The purpose of this policy is to establish procedures to follow to protect patient medical and financial information in compliance with the Red Flags Rules issued pursuant to the Fair and Accurate Credit Transactions Act.

#### **II. POLICY**

It is the policy of [INSERT NAME OF PRACTICE] to identify and detect relevant patterns, practices, and activities that are Red Flags indicating possible medical identity theft, to respond appropriately to those Red Flags, and to correct or mitigate the harm suffered by any person whose information is used unlawfully.

#### **III. DEFINITIONS**

##### **A. Covered Account**

A covered account is an account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk to patients or to the safety and soundness of the practice from identity theft. An account includes an extension of credit, such as the deferred payment of a deductible, copayment, coinsurance amount, etc.

##### **B. Medical Identity Theft**

Medical Identity Theft occurs when a person uses the identity of another person to obtain medical goods or services or to make false claims for medical goods or services.

##### **C. Personal Identifying Information**

Personal identifying information is a person's first and last name in combination with any information that could be used to access a person's financial resources, including but not limited to, the person's Social Security Number, driver's license, passport, state identification card, bank account numbers, credit card numbers, personal identification numbers, and passwords.

#### **D. Red Flags**

Red Flags are patterns, practices, and activities that indicate possible medical identity theft.

#### **E. Security Breach**

A security breach occurs when a person gains unauthorized access to a patient's records or data containing personal identifying information, where the information is used or intended to be used for an unlawful purpose.

### **IV. PROCEDURES**

#### **A. Identification of Red Flags**

The following is a list of Red Flags that we must look for during daily operations. Each of us has been given a copy of this program and shall keep a copy in his or her work area for reference.

1. A fraud or active duty alert that is included in a patient's consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a patient, such as:
  - a. A recent and significant increase in the volume of inquiries;
  - b. An unusual number of recently established credit relationships;
  - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
  - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
5. Documents provided for identification by a patient appear to have been altered or forged.
6. The photograph or physical description on identification presented by a patient is not consistent with the appearance of the patient.

7. Other information on the identification is not consistent with information provided by the patient.

8. Other information on the identification is not consistent with readily accessible information that is in our files, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

10. Personal identifying information provided is inconsistent when compared against external information. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File. The following numbers indicate an invalid SSN:

i. The first three digits are 000, 666, are above 772, or are in the 800 or 900 ranges.

ii. The fourth and fifth digits are 00.

iii. The last four digits are 0000.

11. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the practice. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

12. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the practice. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

13. The SSN provided is the same as that submitted by other persons opening an account or other patients.

14. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other patients.

15. The person opening the covered account or the patient fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

16. Personal identifying information provided is not consistent with personal identifying information that is on file with the practice.

17. The person opening the covered account or the patient cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

18. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, nonpayment when there is no history of late or missed payments.

19. Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.

## **B. Detection of Red Flags**

To detect the Red Flags listed above, we must follow these procedures to verify the identity of each patient.

1. When a patient calls to schedule an appointment, the staff member making the appointment must remind the patient to bring photo identification and an insurance card to the appointment.

2. When a patient arrives for an appointment, a staff member must request photo identification and an insurance card at the time of registration. If the patient does not have photo identification:

i. For new accounts, the patient must provide photo identification to receive services (unless the patient requires emergency services);

ii. For existing accounts, the patient must provide two other types of identification, such as credit cards or a social security card, and be able to verify social security number, date of birth, address, and telephone number. The staff member must place a notification in the patient's file that the patient did not provide photo identification, and the patient will be

required to bring such identification to the next appointment to receive services.

3. When a patient requests a change of address, the staff member must verify the change of address by requiring the patient to provide either an updated driver's license or another document with the patient's name and updated address, such as a current utility bill.

### **C. Appropriate Response to Red Flags**

The following are actions that we must take when a Red Flag is detected.

1. A staff member who detects a Red Flag should immediately notify his or her supervisor.
2. Any time a Red Flag is detected, the supervisor must mark the patient account associated with that Red Flag accordingly. Every patient account with a Red Flag will be monitored for a period of one year.
3. The Program Administrator must investigate any Red Flag to determine whether the detection could possibly result in the misuse of personal identifying information. If so, then the Program Administrator will take the following actions:
  - i. The Program Administrator must notify the patient in writing of the Red Flag, provide a summary of the incident, and advise the patient to monitor free credit reports and possibly contact the major credit reporting agencies.
  - ii. The Program Administrator may close the patient's account, reopen the patient's account with a new account number, and change any passwords or security codes associated with the account.
  - iii. The Program Administrator will work with the patient and the patient's physician to extract any medical records from the patient's file that do not correspond to the patient's medical history. These medical records will be placed in a Jane or John Doe file, and both files will contain cross-references to the other for tracking purposes.
  - iv. If necessary, the Program Administrator may elect to notify local law enforcement to the extent permitted by the practice's HIPAA policy.
4. If a patient notifies the practice of possible identity theft associated with the patient's account, the Program Administrator must investigate the claim and attempt to mitigate any harm to the patient.

- i. The Program Administrator may request the patient to file a police report and provide a copy to the practice. Alternatively, the Program Administrator may request the patient to provide a Federal Trade Commission Identity Theft Affidavit or a similar affidavit. (See Attachment 3 for a form affidavit)
- ii. Once the patient's claim is verified, the Program Administrator will ensure that the practice ceases any collection activities on the account.
- iii. The Program Administrator will refund any insurance company that has paid for services fraudulently obtained.
- iv. The Program Administrator will work with the patient and the patient's physician to extract any medical records from the patient's file that do not correspond to the patient's medical history. These medical records will be placed in a Jane or John Doe file, and both files will contain cross-references to the other for tracking purposes.
- v. If the identity theft resulted in an adverse report made to a consumer reporting agency in association with the patient account, the Program Administrator will notify the consumer reporting agency that the account was not the patient's responsibility.
- vi. If necessary, the Program Administrator may elect to notify local law enforcement to the extent permitted by the practice's HIPAA policy.
- vii. If the Program Administrator determines that the patient has not been the victim of identity theft, the Program Administrator will advise the patient in writing of the basis for that determination and that the patient is responsible for the payment of the bill.

#### **D. Staff Training**

The Program Administrator will develop a training program to educate staff members on the importance of medical identity theft, how it can affect patients and the practice, and how to comply with the Identity Theft Prevention Program policy and procedures.

#### **E. Business Associate Arrangements**

The Program Administrator will oversee all business associate arrangements to ensure that their policies act in accordance with this Identity Theft Prevention Program policy. The Program Administrator may require the business associate by contract to have Red Flag policies and procedures, and to report any Red Flag incidents to the practice.

**F. Periodic Update of the Identity Theft Prevention Program**

The Program Administrator will reassess the program on an annual basis to determine whether any changes should be implemented. The Program Administrator will consider such factors as any incidents of identity theft that have occurred, changes within the practice such as updated technology or new types of covered accounts, changes in methods of identity theft, and changes in methods of detecting and preventing identity theft. The Program Administrator shall submit an annual report to the Board of Directors that documents the compliance of the practice with the Identity Theft Prevention Program. This report must contain any significant identity theft incident that occurred over the past year, any changes in risk to patients or the practice, and recommendations to improve the Program. The Board must approve all changes made to the program.

**Approved By The Board of Directors of, Members of or (name of sole practitioner owner)**

\_\_\_\_\_  
**[Title]**

\_\_\_\_\_  
**[Title]**

\_\_\_\_\_  
**[Title]**

**Date Reviewed/Revised:** \_\_\_\_\_