

DOYLESTOWN FAMILY MEDICINE, P.C.

IDENTITY THEFT PREVENTION PROGRAM
TEMPLATE

ADOPTED AND EFFECTIVE: APRIL 15, 2009

UPDATED:

I. Adoption of Identity Theft Prevention Program

Doylestown Family Medicine, P.C. ("the Practice") developed this Identity Theft Prevention Program ("the Program") pursuant to the Federal Trade Commission's Red Flags Rule ("the Rule"), 16 C.F.R. §681.2. The Program was developed with the oversight and approval of the Practice's [Board of Directors/Managing Partner/Managing Member] who has determined that our Practice is a Creditor with Covered Accounts (as defined below) and is obligated to comply with the Rule. After due consideration of the Rule's requirements and its guidelines (and including in the Program those guidelines in Appendix A of the Rule that are appropriate), and of the size and complexity of the Practice's operations and systems, and the nature and scope of the Practice's activities, the [Board/Managing Partner/Managing Member] determined that this Program is reasonable and appropriate for the Practice and, therefore, approved this Program on the day of , 2009.

II. Program Purpose and Definitions

A. Fulfilling the Obligations of the Rule

Under the Rule, every "Creditor" with "Covered Accounts" is required to establish an Identity Theft Prevention Program tailored to the size, complexity and nature of its operations. The Program must contain policies and procedures

reasonably designed to:

1. Identify relevant "Red Flags" for new and existing "Covered Accounts" and incorporate those Red Flags into the Program.
2. Be able to detect Red Flags that have been incorporated into the Program.
3. Respond appropriately to any Red Flags that are detected in order to prevent and mitigate "Identity Theft."
4. Update the Program periodically to reflect changes in risks to our patients and to the safety and soundness of our Practice from Identity Theft.

B. Definitions of Terms used in the Program

Account means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes, including an extension of credit.

A Covered Account is:

- i. an account that a creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; and
- ii. any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers (our patients) of, or to the safety and soundness of the creditor from, identity theft.

Credit is an arrangement by which a person or entity defers payment of debts or accepts deferred payments for the purchase of services or property.

A Creditor is any person or entity who:

- i. regularly extends, renews or continues credit;
- ii. regularly arranges for the extension, renewal or continuation of credit;
or
- iii. any assignee of an original creditor who participates in the decision to extend, renew or continue credit.

Identifying Information is defined under the Rule as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internal Protocol Address, or routing code.

Identity Theft is fraud committed using the identifying information of another person, which can be medical identity theft and/or financial identity theft.

Program Administrator is the Practice's administrative personnel charged with the implementation of the Program (which may be one or more persons and may be the Practice's HIPAA Privacy Officer).

Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft in connection with a covered account.

Service Provider means a person or entity that provides a service directly to a creditor.

III. Policies and Procedures

A. Identification of Red Flags

Because our Practice regularly extends Credit to patients by establishing an account that permits multiple payments, our Practice is a Creditor offering Covered Accounts.

Commentary to the Rule states that "creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk."

In order to identify relevant Red Flags, our Practice considers the types of accounts it offers and maintains, the methods it provides to open its accounts, the methods it uses or provides to access its accounts, and its previous experience with Identity Theft.

The Practice has identified the following Red Flags for our Program:

1. Alerts, Notifications and Warnings Received from Consumer Reporting Agencies or Service Providers of the Practice

a. Report of fraud or other alert accompanying a credit or consumer report

b. Notice of a credit freeze in response to a request for a consumer report

c. Report, such as from one of our Service Providers, indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of a patient account

2. Suspicious Documents

a. Identification document that physically appears to be forged, altered or otherwise not authentic

b. Identification document on which a person's photograph or physical description is not consistent with the person presenting the document

c. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance (unless the Practice can confirm that there is a legitimate reason for the absence of such documentation)

d. Other document containing information that is not consistent with existing patient information (such as if a person's signature appears forged, based on previous instances of the person's signature on file)

3. Suspicious Personal Identifying Information

a. Identifying information presented that is inconsistent with other information the patient provides (e.g., inconsistent birth dates)

b. Identifying information presented that is inconsistent with other sources of information (e.g., an identification number presented that does not match a number on the person's insurance card)

c. Identifying information presented that is the same as information shown on other documents that were found to be fraudulent

d. Identifying information presented that is consistent with fraudulent activity (e.g., invalid phone number or fictitious billing address)

e. Identifying information presented that is the same as information provided as identifying information by another patient

f. A patient fails to provide complete identifying information on any patient information form when reminded to do so and the Practice is not prohibited by law from requiring the information be provided

g. A patient provides identifying information that is not consistent with the information the Practice has on file for the patient

4. Suspicious Account or Medical Record Activity

a. Payments stop on an otherwise consistently up-to-date account

b. Mail sent to the patient is repeatedly returned as undeliverable

c. Breach in the Practice's computer system security

d. Unauthorized access to or use of Covered Account information

e. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient, e.g., discrepancies in age, race, blood type or other physical descriptors

5. Alerts from Others

a. A complaint or question from a patient based on the patient's receipt of:

i. A bill for another individual

ii. A bill for a product or service that the patient denies receiving

iii. A bill from a health care provider that the patient never patronized

iv. A notice of insurance benefits or Explanation of Benefits for health services never received

b. A complaint or question from a patient about the receipt of a collection notice from a bill collector

c. A complaint or question from a patient about information added to a credit report by the Practice or the patient's insurer

d. A dispute of a bill by a patient who claims to be the victim of any type of Identity Theft

e. A patient or insurance company report that coverage for legitimate medical services is denied because insurance benefits have been depleted or a lifetime cap has been reached

f. A notice or inquiry from an insurance fraud investigator regarding a patient's account (which could indicate internal or external Identity Theft)

g. A notice or inquiry from a law enforcement agency regarding possible Identity Theft in connection with a Covered Account held by the Practice

h. A notice from a victim of Identity Theft regarding possible Identity Theft in connection with a Covered Account held by the Practice

B. Detecting Red Flags

1. New Accounts - In order to detect any of the Red Flags identified above associated with the opening of a new Covered Account, Practice personnel will take the following steps to obtain and verify the identity of the person opening the account:

a. Require certain identifying information such as: name, date of birth, residential or business address, insurance card, employer name and address, driver's license or other identifying information.

b. Actually verify the patient's identity by reviewing the identifying information presented and contacting the patient's insurer, if appropriate.

2. Existing Accounts - In order to detect any of the Red Flags identified above for an existing account, Practice personnel will take the following steps to monitor the transactions and activity on an account, in compliance with our Practice's HIPAA Privacy policies and procedures:

a. Verify the identification of a patient who requests information (in person, via telephone, via facsimile, via email)

b. Verify the validity of requests to change a billing address

c. Verify changes in credit card or other information given for purposes of billing and payment

C. Preventing and Mitigating Identity Theft

In the event Practice personnel detect any identified Red Flags, the Practice shall take

one or more of the following steps, depending on the Red Flag detected and on the degree of risk posed by the Red Flag:

1. Prevent and Mitigate

- a. Notify the Program Administrator who may determine it is necessary to contact the Practice's legal counsel for determination of the appropriate step(s) to take
- b. Comply with state and federal requirements related to a breach of computer security
- c. Contact the patient, in compliance with applicable law
- d. Notify law enforcement, in compliance with applicable law
- e. Continue to monitor an account for evidence of Identity Theft
- f. Change any passwords or other security devices that permit access to a Covered Account
- g. Not open an account for a new patient if a Red Flag is detected in relation to such account
- h. Place a hold on further transactions related to an account for which a Red Flag has been detected
- i. Not attempt to collect on an account
- j. Determine that no response is warranted under the circumstances

2. Protect Patients' Identifying Information

The Practice's HIPAA Privacy and Security Program will be utilized, and updated along with this Program, if necessary, to further prevent the likelihood of Identity Theft occurring with respect to Practice accounts.

3. Protecting and Correcting Medical Information

If our Practice determines that medical Identity Theft has occurred, there may be errors in the patient's chart as a result. Fraudulent information may have been added to a pre-existing chart, or the contents of an entire chart may refer only to the health condition of the identity thief, but under the victim's personal identifying information. In such cases, our Practice shall take appropriate steps to avoid mistreatment due to the fraudulent information, such as file extraction, cross-referencing charts, etc.

D. Program Updates

The Program Administrator will periodically, but no less than annually, review and update this Program to reflect changes in risks to patients and the soundness of the Practice in protecting against Identity Theft, taking into consideration the Practice's experience with Identity Theft occurrences, changes in methods of how Identity Theft is being perpetrated, changes in methods of detecting, preventing and mitigating Identity Theft, changes in the types of accounts the Practice offers, and changes in the Practice's business relationships with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program are warranted. The Program Administrator will present any recommended changes to the [Board/Managing Partner/Managing Member], which will make a determination whether to accept, modify or reject the recommended changes to the Program.

IV. Program Administration

A. Oversight of the Program

The Practice [Board of Directors/Managing Partner/Managing Member] is responsible for the development, implementation and updating of this Program and will approve the initial Program, as well as any updates. The Program Administrator is responsible for taking steps to ensure appropriate training of Practice personnel

regarding the Program, receipt and review of reports regarding the detection of Red Flags, determining (with the assistance of the Board/Partner/Member and/or legal counsel) the steps for preventing and mitigating Identity Theft when a Red Flag is detected, and recommending updates to the Program.

B. Staff Training and Reporting

Practice personnel whose role requires their participation in implementing the Program will be trained by or under the direction of the Program Administrator. Training shall cover the Red Flags identified in the Program, detecting Red Flags, and reporting and responding to detected Red Flags. The Program Administrator shall report annually to the [Board/Partner/Member] on the Practice's compliance with the Rule in terms of effectiveness of addressing Identity Theft, service provider arrangements, significant incidents involving Identity Theft and the Practice's response, and recommendations for material changes to the Program.

C. Oversight of Service Provider Arrangements

The Practice will require, by written contract, that service providers that provide services or perform activities on our Practice's behalf in connection with a Covered Account have policies and procedures in place designed to detect, prevent and mitigate the risk of Identity Theft in regard to the Covered Accounts. If the service provider is a HIPAA Business Associate of the Practice, the Business Associate Agreement with that service provider shall be amended to incorporate the above requirements.

V. State Laws and Regulations

Many states have their own rules which must also be implemented as part of your identity theft prevention program. You must determine whether your state has such rules and, if so, incorporate them into your identity theft prevention program.

