

**RED FLAG RULES
IDENTITY THEFT PREVENTION PROGRAM AND POLICY**

PURPOSE: The purpose of the Interventional Cardiologists of Gainesville, PA (“IVC”) Red Flag Rules Identity Theft Prevention Program and Policy (the “Policy”) is to establish a program to detect, to prevent and to mitigate identity theft in connection with patient accounts maintained by IVC, as required by The Fair and Accurate Credit Transactions Act of 2003.

DEFINITIONS: The following definitions shall apply to terms used within this Policy:

Account – A continuing relationship established by a person with IVC to obtain a health care service or any patient account with which there is a reasonably foreseeable risk of identity theft.

Personal Identifying Information – Includes an individual’s first name or first initial and last name in combination with the following:

- a) Social Security Number;
- b) Driver’s License Number;
- c) Account Number, Credit Card Number or Debit Card Number in combination with any security code, access code or password that would allow access to a financial account of the person; or
- d) Federal or State Identification Cards.

Red Flag – A pattern, practice or specific activity that indicates the potential for identity theft.

Service Provider – A person or entity who provides services directly to IVC. For example, a vendor who maintains or provides software used in connection with Accounts is a service provider.

PROCEDURES:

I. Identification of Red Flags

Potential Red Flags may be identified as a result of the following:

Alerts, Notifications or Warnings

- a) Alerts, notifications or other warnings from consumer reporting agencies, fraud detection services or an insurance company concerning a fraud investigation;
- b) Notice from patients, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with Accounts;

**RED FLAG RULES
IDENTITY THEFT PREVENTION PROGRAM AND POLICY**

Suspicious Documents

- c) Documents provided for identification appear to have been forged;
- d) The photograph or physical description on the identification is not consistent with the appearance of the patient presenting the identification;
- e) Other information on the identification is not consistent with information provided by the person opening the new Account or presenting the identification;
- f) An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled;

Suspicious Personal Identifying Information

- g) Personal Identifying Information provided is inconsistent when compared against external information sources used by IVC (*e.g.*, the social security number has not been issued or is listed in the Social Security Administration's Death Master File);
- h) Personal Identifying Information provided by the patient is inconsistent with other information provided by that patient (*e.g.*, there is a lack of correlation between the patient's social security number range and their date of birth);
- i) Personal Identifying Information provided is associated with a known fraudulent activity as indicated by internal or third-party sources used by IVC (*e.g.*, the address provided is the same as an address that has been identified as fraudulent);
- j) Personal Identifying Information provided is of a type commonly associated with fraudulent activity (*e.g.*, the address is fictitious or the phone number is invalid);
- k) The social security number provided is the same as one submitted by other persons opening a new Account);
- l) 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 persons opening an Account);
- m) The patient fails to provide all of the required Personal Identifying Information (*e.g.* patient has insurance number but can never produce an insurance card or other insurance documentation or verification);

Unusual Use of, or Suspicious Activity Related to, the Account

- n) Patient complaints or questions concerning a bill for another individual or for services the patient never received;
- o) Patient record shows medical treatment that is inconsistent with their history and physical information;

RED FLAG RULES
IDENTITY THEFT PREVENTION PROGRAM AND POLICY

- p) Patient complaints or questions about collection notices from a bill collector for services never received;
- q) Patient or patient's insurance company reports a denial of patient's coverage because depletion of patient's benefits or patient reached their lifetime cap;
- r) Dispute of bill by patient claiming to be the victim of identity theft; or
- s) IVC is notified that the patient is not receiving paper Account statements in the mail.

II. Detection, Investigation of and Response to Potential Identity Theft

A. Detection

1. Opening New Accounts and Existing Accounts

IVC will use its best efforts to obtain identifying information about, and to verify the identity of, a person opening an Account or making payments on an existing Account. To that end, personnel responsible for establishing and maintaining patient Accounts shall ask for a valid driver's license or other photo ID, the patient's current insurance card, and if the photo ID does not contain the patient's current address, utility bills to show the patient's current address. When the patient arrives for his or her appointment, the patient will be asked to produce the information listed above unless the patient has been seen in the past six (6) months. Further, personnel should actively monitor transactions and verify the validity of any change in address requests.

2. External or patient notifications

IVC may receive notice of fraud investigations or Red Flags from external sources, such as consumer reporting agencies, fraud detection services, insurance companies, law enforcement agencies, patients, victims, and other persons.

B. Investigations

If a Red Flag is detected, IVC shall conduct an investigation to determine if the breach or detection of a Red Flag could result in the misuse of any Personal Identifying Information. If an individual detects a Red Flag, he or she must send a written report within one (1) business day of the detection to the Privacy Officer. Within two (2) business days of the report, the Privacy Officer will establish the protocol for investigating and responding to the detected Red Flag. All investigations should be completed within seven (7) business days of the initial report.

**RED FLAG RULES
IDENTITY THEFT PREVENTION PROGRAM AND POLICY**

C. Response

The appropriate response to a detected Red Flag should be commensurate with the degree of risk posed. In determining the appropriate response to detection of a Red Flag, IVC should consider any aggravating factors that may heighten the risk of identity theft. If the investigation leads to the conclusion that identity theft may have occurred, appropriate responses may include the following:

- a) Monitoring an Account for evidence of identity theft;
- b) Notifying the patient either in writing or by e-mail. This notification must include a local or toll-free number the individual may use to contact IVC and receive information about toll-free numbers and addresses for major credit reporting agencies;
- c) Changing any passwords, security codes or other security devices that permit access to an Account;
- d) Correcting the patient's Account and medical records;
- e) Filing an alert on the Account;
- f) Reopening an Account with a new Account number;
- g) Not opening a new Account or closing an existing Account;
- h) Notifying local law enforcement;
- i) Not attempting to collect on an Account or not selling the Account to a debt collector;
- j) Determining that no response is warranted under the circumstances.

III. Oversight of Service Providers

If IVC engages a Service Provider to perform an activity in connection with one or more Accounts, IVC shall include in its written arrangement with the Service Provider that the activity of the Service Provider shall be conducted in accordance with reasonable policies and procedures designed to detect, to prevent and to mitigate the risk of identity theft.

IV. Risk Assessment

On not less than a yearly basis, IVC shall conduct a risk assessment to ascertain the reasonably foreseeable risk of identity theft for patients who have Accounts with IVC. The risk assessment shall take into account (a) the types of Accounts offered or maintained by IVC, (b) the methods IVC provides to open Accounts, (c) the methods IVC utilizes to access Accounts, and (d) IVC's previous experiences with identity theft.

**RED FLAG RULES
IDENTITY THEFT PREVENTION PROGRAM AND POLICY**

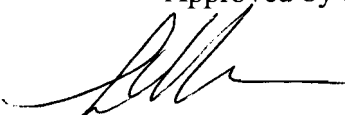
ADMINISTRATION: The Privacy Officer of IVC shall have oversight responsibility for this Policy. The Privacy Officer shall assign specific responsibility for implementation of the Policy, review reports detailing any investigations into possible identity theft, and approve material changes to the Policy.

The Privacy Officer shall report material matters related to the Policy (e.g., the general effectiveness of the Policy, significant incidents involving identity theft and response, or recommended material changes to the program) to the Board of Directors annually.

POLICY UPDATES: This Policy should be updated based on (a) IVC's experiences with identity theft, (b) changes to the methods of detecting, preventing or mitigating identity theft, (c) changes in the types of Accounts maintained by IVC, or (d) changes in any of the IVC's business arrangements with third-party insurers or patients.

RELATED POLICIES: This Policy shall supplement and incorporate into it by reference IVC's applicable policies and procedures pertaining to the Health Insurance Portability and Accountability Act.

Approved by the Board of Directors of IVC as of May 18, 2009.



By: Lonan McDowell
Its: CEO