Step Alive Foot & Ankle Center
Red Flag Rule/Identity Theft Compliance Program
Effective Date: Monday, July 27, 2009

It is the policy of Step Alive Foot & Ankle Center to follow all Federal and state laws and reporting requirements regarding identity theft. The effective date of this program is Monday, July 27, 2009.

Background

Companies that extend credit must have a written program to prevent identity theft, as well as to detect and respond to warning signs ("red flags") of such thefts, as set forth in the Fair and Accurate Credit Transactions Act of 2003. Physician practices bill patients and insurance companies and are thus considered creditors by the Federal Trade Commission. Therefore, we must comply with this Act.

Our policies and procedures for identity theft prevention and detection are set forth in this program. "Red Flags" are warning signs that suggest possible identity theft; a red flag may be a pattern of suspicious behavior or a specific instance. This program sets forth how The Step Alive Foot & Ankle Center will (1) **identify** red flags, (2) **detect** red flags, and (3) **respond** to probable or actual identity theft.

Please be advised: the majority of identity thefts are 'inside jobs' that can be attributed to the actions of an employee or business associate. Any employee who violates this program will be summarily discharged and prosecuted to the full extent of the law. We will terminate our relationship with any business associate that violates this program and assist law enforcement in prosecuting the business associate to the full extent of the law. The Step Alive Foot & Ankle Center is fully committed to preventing the identity theft of its patients and its employees.

Identifying Red Flags

There are several warning signs that suggest the possibility of identity theft:

- Complaints or inquiries from a patient based upon the patient's receipt of:
    - A statement for another patient;
    - A statement for services the patient denies receiving;
    - A statement from a healthcare provider the patient denies ever seeing
    - A notice or call from a collection agency for services the patient denies receiving; or
    - An Explanation of Benefits for services the patient denies receiving
- Patient records showing medical treatment that is inconsistent with the presenting patient's medical history
- Suspicious documents, such as a forged or suspicious driver's license or health insurance card
- A patient who has an insurance number but never produces a card or documentation
- A relative or caregiver who states they have power of attorney or custody for a patient but who cannot provide supporting documentation
- A patient or insurance company report that coverage is denied because insurance benefits have been depleted or an annual or lifetime cap has been reached
- A patient who looks noticeably different form their photo ID
- Alerts, notifications or warnings from a consumer reporting agency
- Notification from patients, victims of identity theft, law enforcement authorities or others about possible identity theft associated with our patients/patient accounts

Should an employee observe any of these warning signs, they should report the suspicious activity immediately.

Detecting Red Flags

The Step Alive Foot & Ankle Center will follow several procedures to verify the identities of our patients.

1. When making an appointment for a patient, we will ask the patient to bring the following documents to her/his appointment:
    a. Her/his driver's license or other photo ID
    b. Current health insurance card
    c. If the address on the patient's photo ID is different from their present address, a copy of a utility bill or other correspondence showing their current address

2. At check-in, we will ask patients to produce these same documents. Established patients who are known to the front office will not be required to produce such identification. We will monitor for red flags of concern by taking the following steps:
    a. When new patients are checked in for the first time, we will verify that the patient/guarantor is the person shown in the patient/guarantor's photo ID
    b. We will study drivers licenses and insurance cards for signs of potential tampering or falsification
    c. We will be alert for other information on the photo ID or insurance card that is not consistent with information provided by the patient or responsible party (such as a different date of birth or social security number)
    d. We will be alert to changes in the signatures of patients and guarantors.
    e. When a patient or guarantor cannot produce requested documents or basic information, the front office staff will report suspicious activity
3. Returned patient mail and statements will be monitored for discrepancies, including but not limited to, the following:
    a. Returned mail on new patients who received services in our office
    b. Returned mail on an existing patient who continues to come in for services
    c. Indication of a bogus address, such as a mail drop, business address, or prison
4. Our business office/billing staff will be on special alert for financial red flags, including but not limited to the following:
    a. A person questioning a statement for services they state they did not receive
    b. A patient or guarantor who is not receiving paper account statements
    c. The patient or guarantor notifies us of unauthorized charges or transactions in connection with a patient's covered account
    d. A complaint or question from a patient about information added to a credit report by the practice
    e. Insurance denials associated with the patient maxing out annual or lifetime benefit caps
    f. Information that is not consistent with readily accessible information on file, such as a signature or a recent check
    g. Personal identifying information provided is inconsistent when compared against external information sources, such as the insurance company or collection agency. For example:
        i. The address does not match any address on record
        ii. The Social Security Number (SSN) has not been issued
        iii. Personal identifying information provided by the patient or guarantor is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
    h. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources. For example:
        i. The address on an account is the same as the address previously provided on a fraudulent account
        ii. The phone number on an account is the same as the number previously provided on a fraudulent account.
    i. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources. For example:
        i. The address on an application is fictitious, a mail drop, or prison
        ii. The phone number is invalid, or is associated with a pager or answering service
        iii. The SSN provided is identical to that of another patient or is invalid.
        iv. 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 patients/guarantors
        v. The patient or guarantor fails to provide all required personal identifying information on an account or fails to respond to numerous notifications regarding incomplete information
    j. A patient account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example

   i. Non-payment when there is no history of late or missed payments
   ii. A material increase in the use of available credit (high charges accumulating on an account)
5. Providers and nursing staff will be on alert for discrepancies that occur during the course of patient care,
   a. Patient's account of basic information (e.g., date of birth, allergies, medications, family medical history) is inconsistent with previously documented care
   b. Patient's current medical issue conflicts in an illogical way with what is already documented for the patient's history
6. Administration's responsibility includes, but is not limited to the following:
   a. Training the staff
   b. Annual updates to the program
   c. Ensuring that applicable Business Associate contracts are updated to reflect their compliance with the Red Flag Rules
   d. Ensuring that our business associates protect the identities of our patients and our staff
7. All providers and staff are responsible for the following:
   a. Logging off of computers before leaving for the day
   b. Notifying a supervisor immediately if you see someone transferring information from our system to a storage device, such as a "thumb drive"
   c. Notifying a supervisor immediately of any suspicious behavior on the part of a patient, business associate, or employee.

Responding to Red Flags

1. Staff members are required to immediately notify a supervisor and complete the 'Notification of Suspected Identity Theft' form (please see attached form)
2. Supervisors are responsible for investigating further to determine the extent of concern about the red flag and documenting the event and their finding in the patient's record.
3. Action taken may include the following:
   a. Interviewing the patient or guarantor further to substantiate or rule out the concern and asking them to complete the 'ID Theft Affidavit' form (please see attached) and the 'Fraudulent Account Statement' form (please see attached). Instructions for completing these forms and a cover letter to be sent to patients/guarantors are attached.
   b. Flagging the patient/account for further monitoring
   c. Restricting the account so that only a supervisor can make changes and/or respond to future inquiries
   d. Deferring non-urgent services until the matter is cleared up
   e. Closing an account and/or opening a new one
   f. Not trying to collect on an account in instances when the individual being billed has been a proven victim of identity theft
   g. Determining that no response is warranted at that time
4. When it is clear or reasonably certain that the practice has encountered a legitimate red flag, then the Administrator is responsible for contacting the police and the patient(s) involved.

This program shall be reviewed and updated annually to remain current with the practice's operations and applicable environmental developments.

This program is hereby approved.

Electronic Signature: Dr. Thomas F. Vail, DPM
Step Alive Foot & Ankle Center

The Step Alive Foot & Ankle Center

BOARD RESOLUTION

IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, it is the policy of The Step Alive Foot & Ankle Center to require compliance with the laws and regulations relating to the privacy and confidentiality of patient health and medical information and to assure that our functions are pursued in a manner consistent with the letter and the spirit of the laws.

NOW, THEREFORE, BE IT RESOLVED, that The Step Alive Foot & Ankle Center is committed to compliance with such laws and regulations and intends to assure that its operations, as carried out by its employees and other staff and contractors, are conducted in compliance with such laws and regulations;

BE IT FURTHER RESOLVED, that the written Identity Theft Prevention Program attached hereto is hereby approved and adopted.

BE IT FURTHER RESOLVED, that The Step Alive Foot & Ankle Center requires that all members of the workforce, including employees, volunteers, trainees, and other persons whose performance of work is under the direct control of The Step Alive Foot & Ankle Center adhere to and comply with the policies and requirements of the Identity Theft Prevention Program.

ADOPTED this ____27th__ day of ___July____, 2009.

Electronic Signature: Dr. Thomas F. Vail, DPM
Step Alive Foot & Ankle Center