

**FACILITY: ASP OF DICKINSON, LLP
d/b/a MAINLAND SURGERY CENTER**

**TITLE: IDENTITY THEFT PREVENTION
PROGRAM (Red Flags Rules)**

P&P #: AD 079

PAGE 1 of 5

EFFECTIVE DATE: July 20, 2009

REPLACES: New

DISTRIBUTION: All Departments

Purpose:

The primary purpose of the rule is to protect against the establishment of false accounts and ensure existing accounts are not being manipulated.

Policy:

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Definitions:

“**Identity Theft**” means a fraud committed or attempted using the identifying information of another person without authority.

“**Identifying Information**” means any name or number that may be used alone or in conjunction with any other information, to identify a specific person, including any:

- Name, Social Security Number, Date of Birth, Official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice point, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code

“**Credit**” the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

“**Creditor**” any person who regularly extends, renews or continues credit: or any assignee of any original creditor who participates in the decision to extend, renew, or continue credit

Procedure:

Risk Assessment

The Mainland Surgery Center has conducted an internal risk assessment by

- Assessing the existing identity theft risk for new and existing accounts;
- Using the risk assessment to select measures that may be used to detect attempts (red flags) to establish fraudulent accounts;
- Identifying procedures for employees to prevent the establishment of false accounts and procedures for employees to implement if existing accounts are being manipulated;
- Training the appropriate employees on the program’s policies and procedures;
- Updating the plan annually with review and approval by the governing body.

Detection (Red Flags at Registration)

The Mainland Surgery Center adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Patient cannot produce a valid insurance card at the time of service, or presents an insurance number without an insurance card
- Address listed on patient's insurance policy does not match the address on the patient's driver's license
- Identification documents appear to be altered or forged
- Photo and physical description do not match appearance of patient
- Other information is inconsistent with information provided by patient
- Other information provided by patient is inconsistent with information on file.
- Patient provides personal identifying information that is inconsistent when compared against external information sources or that is associated with known fraudulent activity.
- Patient provides a P. O. Box or a mail drop as a home address.
- Address discrepancy: address discrepancies between information provided by the patient and the credit report or other data (internal files, return address on envelope is different than internal files or other third party).
- Personal information provided is inconsistent with information on file for patient
- Patient cannot provide information requested beyond what could commonly be found in a purse or wallet

Detection (Red Flags Patients)

- Patient received a bill for another patient.
- Patient received a bill or EOB for services the patient denies having or for treatment from a provider the patient did not patronize.
- Complaint or question from a patient about receiving a collection notice from a bill collector, or about information being added to their credit report by a healthcare provider or insurer.
- Patient who has a previous history of identity theft disputes a bill.

Suspicious Events, Patterns, or Activities

- Records indicate medical treatment is not consistent with physical examination or medical history.
- Insurance claims for legitimate services are denied due to depletion of insurance benefits or because lifetime cap is reached.
- The Surgery Center or patient receives a notice or inquiry from an insurance fraud investigator.
- A new revolving credit account is used in a manner commonly associated with known fraud patterns.
- Mail sent to the patient is repeatedly returned as undeliverable, although transactions continue to be conducted in connection with the patient's account.
- An alert, notification or warning is received from a credit reporting company regarding this patient.

Response

- Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the Business Office Manager.
- Ask patient for additional documentation; minimum of two identifying documents such as:
 - Driver's License
 - Insurance Card
 - Government Issued Identity Card
 - Credit Card with photo

- Utility bills
- Notify Business Office Manager when any staff person becomes aware of a suspected or actual fraudulent use of a patient identity.
- Notify law enforcement of any attempted or actual identity theft.

Personal Information Security Procedures:

The Mainland Surgery Center adopts the following security procedures.

- Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.
- Only specially identified employees with a legitimate need will have keys to the room and cabinet.
- Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
- Employees will not leave sensitive papers out on their desks when they are away from their workstations.
- Employees store files when leaving their work areas
- Employees log off their computers when leaving their work areas
- Employees lock file cabinets when leaving their work areas
- Employees lock file room doors when leaving their work areas
- Access to offsite storage facilities is limited to employees with a legitimate business need.
- Any sensitive information shipped using outside carriers or contractors will be encrypted
- Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
- Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the Surgery Center.
- No visitor will be given any entry codes or allowed unescorted access to the office.
- Access to sensitive information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different.
- Passwords should not be shared or posted near workstations.
- Password-activated screen savers will be used to lock employee computers after a period of inactivity.
- When installing new software, immediately change vendor-supplied default passwords to a more secure password.
- Sensitive consumer data will not be stored on any computer with an Internet connection.
- Sensitive information that is sent to third parties over public networks will be encrypted.
- Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.
- Email transmissions within the business will be encrypted if they contain personally identifying information.
- Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
- When sensitive data is received or transmitted, secure connections will be used.

- Computer passwords will be required.
- User names and passwords will be different.
- The use of laptops is restricted to those employees who need them to perform their jobs.
- Laptops are stored in a secure place.
- Laptop users will not store sensitive information on their laptops.
- Laptops which contain sensitive data will be encrypted.
- Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
- If a laptop must be left in a vehicle, it is locked in a trunk.
- The computer network will have a firewall where your network connects to the Internet.
- Any wireless network in use is secured.
- Maintain central log files of security-related information to monitor activity on your network.
- Monitor incoming traffic for signs of a data breach.
- Monitor outgoing traffic for signs of a data breach.
- Check references or perform background checks before hiring employees who will have access to sensitive data.
- New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
- Access to patient's personal identify information is limited to employees with a "need to know."
- Procedures exist for making sure that workers who leave your employ no longer have access to sensitive information.
- Annual in-service provided to all staff.
- Employees will be alert to attempts at phone phishing.
- Employees are required to notify the Business Office Manager immediately if there is a potential security breach, such as a lost or stolen laptop, login and password breach.
- Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
- Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
- Paper shredders / shred bins are available for disposal of all sensitive data.
- Any data storage media will be disposed of by shredding, punching holes in, or incineration.

Review and Approval

This plan has been reviewed and adopted by the Surgery Center Governing Board of Directors and will review the plan annually.

Surgery Center employees have been trained on the contents and procedures of this prevention program.

A report will be prepared annually and submitted to the governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any

third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

Reference

16 C.F.R. §681

16 C.F.R. §603.2

Federal Trade Commission: Fighting Fraud with the Red flag Rule – A How-To Guide for Business

www.ftc.gov/redflagrule

End of Policy & Procedure