UNIVERSITY SPECIALTY CLINICS®

IDENTITY THEFT PREVENTION AND DETECTION
PROGRAM, POLICY, AND PROCEDURES

POLICY:

The Federal Trade Commission (FTC), along with federal bank regulators, adopted regulations implementing the FACT Act (the Red Flags Rule) that require creditors to adopt a written Identity Theft Prevention Program. University Specialty Clinics® is a creditor subject to the FTC's Red Flags Rule and has established an Identity Theft Prevention and Detection Program (Program) and Policy and Procedures to detect, prevent, and mitigate identity theft of our patients' identifying information in connection with opening a covered account or any existing covered account.

POLICY EFFECTIVE DATE: May 1, 2009

APPLIES TO: University Specialty Clinics® and its Service Providers

PURPOSE:

The Identity Theft Prevention and Detection Program promotes:

1. Identification of the relevant patterns, practices, and specific forms of activity that are Red Flags signaling possible identity theft
2. Implementation of policies and procedures for detecting Red Flags, obtaining identifying information about and verifying the identity of a person opening a covered account, and for existing accounts, addressing the detection of Red Flags such as by authenticating customers and monitoring transactions
3. Identification of steps University Specialty Clinics® can take to respond to any Red Flags that are detected to prevent and mitigate identity theft
4. Creation of a system for periodic updates to the Program to reflect changes in risks to customers, and provide for administrative oversight to the Program

PROCEDURES:

I. The Program

A. Oversight

The Privacy Office and the Legal Office will provide oversight for the Red Flags initiative.

B. Reports

The Director of Legal Affairs will review and evaluate Program effectiveness and report annually to the Privacy and Security Advisory Committee (PSAC). The annual report shall discuss material matters related to the Program and evaluate issues related to:

1. The effectiveness of the Policy and Procedures in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts
2. Service Provider (Business Associate) arrangements
3. Significant incidents involving identity theft and management's response
4. Recommendations for changes in the Program

C. Service Provider Arrangements

University Specialty Clinics® shall exercise appropriate oversight of Service Provider arrangements to ensure that the activity of the Service Provider is conducted in accordance with reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft.

1. University Specialty Clinics® shall notify all Service Providers, in writing, of this Policy and the Service Providers' obligations to implement reasonable policies and procedures that comply with the Red Flags Rule and this Policy. All future Service Provider agreements executed by University Specialty Clinics® and Service Providers shall require the same.
2. University Specialty Clinics® may require, by contract, the Service Provider to report the Red Flags to University Specialty Clinics® and to take appropriate steps to prevent or mitigate identity theft.

D. Training

The Privacy Officer shall train or arrange for the initial training of all appropriate personnel currently employed and all newly hired appropriate personnel within forty-five (45) days of hire.

II. Identifying Relevant Red Flags

The Red Flags are identified as the following:

- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a covered account;
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by University Specialty Clinics®;
- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services

III. Detecting Red Flags

University Specialty Clinics® personnel should exercise due diligence in the detection of a possible Red Flag or identity theft by requesting identifying information at registration or intake points and including a copy of this information in the patient's file and by being alert to other signs that the information offered is not valid. If asked the reason for identifying procedures, personnel should explain that the procedures are "for patient protection to help prevent identity theft."

IV. Preventing and Mitigating Identity Theft

A. Patient Registration

If there is any reason to believe a Red Flag exists or that identity theft has occurred, the University Specialty Clinics® employee should step away from the patient registration area and notify his/her immediate supervisor or the Administrative Director before completing the patient encounter.

B. Discrepancy Reports

If a discrepancy is reported, the person receiving the report should notify his/her immediate supervisor or Administrative Director.

C. Incident Reporting and Response

If the Administrative Director finds that there is a discrepancy that cannot be resolved, the Administrative Director should then contact the Privacy Office or the Legal Office, from where a report will be filed to the Incident Response Team.

DEFINITIONS:

Business Associate - A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Covered Account - 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 customers or the safety and soundness of the creditor from identity theft.

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 defers payment therefore.

Identifying Information - Any name or number that may be used, alone or in conjunction with any other information, to identify a patient, including any: (1) 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; (2) unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation; (3) unique electronic identification number, address or routing code; or telecommunication identifying information or other access device.

Identity Theft - A fraud committed or attempted using the Identifying Information of another person without authority.

Incident Response Team – The University Specialty Clinics® committee that reviews, and coordinates response to, detected or reported HIPAA Privacy, HIPAA Security, and Red Flag incidents.

Patient - For purposes of the Program, an individual with a covered account with University Specialty Clinics®.

Red Flag - A pattern, practice or specific activity involving a patient that indicates the possible existence of identity theft.

Red Flags Regulations - Those final Federal Regulations published by the Federal Trade Commission as "Identity Theft Rules" under 16 CFR part 681.

Service Provider - A business associate that performs an activity in connection with one or more covered accounts that is in a position to identify and report a Red Flag to University Specialty Clinics® in the normal course of business.

University Specialty Clinics® personnel - Any authorized University Specialty Clinics® workforce member who may be in a position to identify and report a Red Flag to University Specialty Clinics® in the normal course of business.