Orthopaedic Associates of Duluth, P.A.
Policies and Procedures
Red Flag Rules
Identity Theft Prevention Program

Purpose: To establish an Identity Theft Prevention Program designed to take reasonable measures to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing account. The Red Flag Rules are intended to ensure the safety of sensitive patient information. The regulations, also called Identity Theft Red Flags Rule, implement part of the Fair and Accurate Credit Transactions (FACT) Act of 2003.

Definitions:

Identity Theft is fraud that is committed using the identifying information of another person, which can be medical identity theft and/or financial without his/her authority.

A Covered Account is defined as an account used mostly for personal, family or household purposes, and involves multiple payments or transactions. A Covered Account is also an account for which there is a foreseeable risk of identity theft.

Creditor is any entity that regularly extends, renews or continuous credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignees of an original creditor who is involved in the decision to extend, renew or continue credit.

A Red Flag alerts you to circumstances that signal a potentially high risk situation. It is a pattern, practice or specific activity that could indicate identity theft in connection with a covered account.

Medical Identity Theft occurs when someone uses a person's name and sometimes other parts of their identity, such as insurance information or Social Security Number without the victims knowledge or consent to obtain medical services or goods, or when someone uses the person's identity to obtain money by falsifying clams for medical services and falsifying medical records to support those claims.

The Program:
Orthopaedic Associates of Duluth, P.A.
is required to have an Identity Theft Prevention Program, there are four required elements:

1. Identify relevant Red Flags for the covered accounts that the creditor Associates of Duluth, P.A.) offers or maintains and incorporate those Red Flags into its program;
2. Detect Red Flags that have been incorporated into its program;
3. Respond appropriately to any Red Flags that are detected;
4. Update the program periodically to reflect changes in risks from identity theft to patients and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing polices and procedures that control reasonably foreseeable risks.

As examples Orthopaedic Associates of Duluth, P.A. would like to implement into the Program the following:

1. Checking patients' photo ID's when medical services are sought, i.e. drivers license, parks pass, college ID.
2. Make a copy of their ID and place it in their chart.
3. When the patient returns, you must ask them for their Drivers License, you will then check to see if the person standing in front of you is identified as the person in the picture in the covered account.
4. Verify the patients address, and home telephone number.
5. If you become suspicious of the person standing in front of you, immediately notify your Team Leader

Administration of the Program:

1. The Office Manager will be responsible for the development, implementation, oversight and continued administration of the program. The Executive Management Board will review and approve the Red Flag Rules Policy Program.
2. The Program will train all staff, as necessary, to effectively implement the Program; and
3 The Program will exercise appropriate and effective oversight of service Provider arrangements.
4. The Program will review all reported incidents prepared by the staff.
5. The identity Theft Red Flag Rules require covered entities to implement a program to detect and appropriately respond to signs of identity theft.

Identification of Relevant Red Flags:

1. The Program includes relevant red flags from the following categories as appropriate:
    - Alerts, Notifications and Warnings received from Consumer Reporting Agencies or Service Providers of the Practice, such as fraud detection services;
    - The presentation of a new patient;
    - The presentation of suspicious documents, on which a persons photograph or physical description is not consistent with the person presenting the document;
    - The presentation of suspicious personal identifying information;
    - The request to change patient information; and
    - Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with the covered accounts.

2. The Program will consider the following risk factors in identifying relevant red flags for covered accounts as appropriate.
    - The types of covered accounts offered or maintained;
    - The methods provided to open covered accounts;
    - The methods provided to access covered accounts; and
    - Its previous experience with identity theft.

3. The Program will incorporate relevant red flags from sources such as:
    - Incidents of identity theft previously experienced;
    - Methods of identity theft that reflect changes in risk; and
    - Applicable supervisory guidance

.

Detection of Red Flags:

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by;

1. Obtaining identifying information about, and verifying the identity of, a new patient, or existing patient (covered account), for example, using the policies and procedures regarding identification and verification set forth in this program.
2. Authenticating patients, monitoring transactions, and verifying the validity of change of address requests in the case of existing patient (covered) accounts.
3. Personal identifying information provided is inconsistent when compared against external information sources.
    a. The address does not match, it could be fictitious
    b. The phone number does not match
    c. The person accessing, or opening the covered account fails to provide proper identification, for example, their photo ID

Response:
The Program will provide appropriate responses to detected red flags to prevent and mitigate identity theft. The response will be depending on the red flag detected and on the degree of risk posed by the Red Flag. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft.
2. Contact the patient;
3. Changing password, security codes, or other security devices that permit access to a covered account;
4. Reopen a covered account with a NEW account number;
5. Not opening a new covered account;
6. Close an existing covered account;
7. Notify local law enforcement; or
8. Determine no response is warranted under the particular circumstances.

Updating the Program:
The program will be updated periodically to reflect changes in risks to patients or the safety and dependability of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the organization offers and maintains;
5. Changes in business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Oversight of the Program:

1. Oversight of the Program shall include:
    a. Assignment of specific responsibility for implementation of the program;
    b. Review of reports prepared by staff regarding compliance; and
    c. Approval of material changes to the program as necessary to address changing risks of identity theft.
2. Staff Training and reporting
    a. Employees whose role requires participation in implementing the

Program will be trained by or under the direction of the CEO. The employees must report to the CEO at least annually on compliance by the organization with the program.

b. The report shall address material matters related to the program and evaluate issues such as:
    i. The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
    ii. Significant incidents involving identity theft and management's response;
    iii. Recommendations for material changes to the program.

Oversight of Service Provider Arrangements:
Orthopaedic Associates of Duluth P.A. will take steps in enforcing policy and procedures in place for all covered accounts, which will be designed to detect, prevent and mitigate risk of identity theft. The Organization will take steps to ensure that the activity of a service provider is conducted in accordance with the reasonable policies and procedures designed to protect all covered accounts.

Duties Regarding Address Discrepancies:
The address discrepancy requirement attaches to any user of a nationwide credit report. The organization will develop policies and procedures designed to enable the organization to form reasonable belief that a credit report relates to the customer for whom it was requested if the organization receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.
Orthopaedic Associates may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the patient;
2. Verification of the address through third-party sources; or
3. Verifying the information in the consumer report provided by the consumer reporting agency with the customer.
4. Other reasonable means.

Conclusion:
Orthopaedic Associates of Duluth, P.A., will train and educate the staff, and create awareness about Identity Theft, and possible Red Flags. If an employee is suspicious, and or receives information about a covered account, they are to notify their Team Leader immediately, The Chief Executive Officer will be notified, and Orthopaedic Associates of Duluth, P.A. will set its response plan in motion when a red flag is raised. Medical Identity Theft is an emerging issue that raises concerns for patients, and we shall detect, prevent and mitigate identity theft in connection with the opening of a covered account, or existing account.

August 1, 2009

Dear Patient,

The Federal Trade Commission (FTC) has released a new rule to protect consumers from IDENTITY THEFT, which is now becoming known as the "Red Flag Rule". The new rule now requires any corporation which extends credit to implement a written identity theft prevention program. Under the FTC's guidelines, physicians who regularly bill their patients for services rendered (including copayments, co-insurance and deductibles) are considered creditors and therefore must comply with the "Red Flag Rules."

As a result, Orthopaedic Associates of Duluth, P.A. will now require the following information from all patients to ensure the identity of the person being seen:

1. Drivers License or state issued form of identification with picture
2. Proof of Insurance

Once we have validated that the patient being seen matches the information provided, we will store this proof in the patient's medical records by taking a photocopy of the identification. This eliminates the need to ask for this information in the future unless something changes.

We regret any inconvenience this may cause. We do ask that you remember that, just like many other institutions, Orthopaedic Associates of Duluth, P.A. must abide by federal law to keep your information protected. As a result, we have very rigid policies and procedures to insure that your records remain confidential and well-safeguarded.

Thank you in advance.