

Orthopaedic Associates, Inc.

Identity Theft Prevention Program

Purpose

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and
2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

The Program

Orthopaedic Associates establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

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

Administration of Program

1. Orthopaedic Associates' Practice Administrator shall be responsible for the development, implementation, oversight and continued administration of the Program.
2. The Program shall train staff, as necessary, to effectively implement the Program; and
3. The Program shall exercise appropriate and effective oversight of service provider arrangements.

Identification of Relevant Red Flags

1. The Program shall include relevant red flags from the following categories as appropriate:
 - a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
 - b. The presentation of suspicious documents such as health insurance ID cards
 - c. The presentation of suspicious personal identifying information;
 - d. The unusual use of, or other suspicious activity related to, a covered account; and
 - e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

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

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

Detection of Red Flags

The Program shall 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 person opening a covered account; and
2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;
2. Contact the customer;
3. Change any passwords, 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 open a new covered account;
6. Close an existing covered account;
7. Notify law enforcement; or
8. Determine no response is warranted under the particular circumstances.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness 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 or maintains;
5. Changes in the 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. Reports shall be prepared as follows:
 - a. Staff responsible for development, implementation and administration of the Program shall report to *Orthopaedic Associates'* Practice Administrator 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. Service provider agreements;
 - iii. Significant incidents involving identity theft and management's response; and
 - iv. Recommendations for material changes to the Program.

Oversight of Service Provider Arrangements

Orthopaedic Associates shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Duties Regarding Address Discrepancies

Orthopaedic Associates shall develop policies and procedures designed to enable the organization to form a reasonable belief that a credit report relates to the consumer 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 consumer;
2. Review of the organization's records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, Orthopaedic Associates shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The organization establishes a continuing relationship with the consumer; and
2. The organization, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

Approved:

Date:

Policies and Procedures: Protecting Patients From Identity Theft

We recognize that identity theft is a crisis in our country, exposing victims to financial loss, credit destruction, business disruption, and confusion of personal information. Medical identity theft, in particular, also may lead to false patient information that could jeopardize the delivery of safe, quality health care.

This office must collect and store our patients' private medical, financial, and personally identifying data. We must therefore be vigilant in protecting the patient information to which we have access.

1. Identity Theft Overview

This office understands that protecting our patients' privacy and all forms of identity theft are integrally related. Accordingly, we take a holistic view of all issues related to patient privacy, including medical, financial, and any other personal information contained in this office's medical, appointment, or billing records.

- a. This office is committed to protecting our patients from identity theft, including medical identity theft.
 - We will comply with all federal and state laws pertaining to identity theft or "Red Flag Rules" such as those pursuant to the Fair and Accurate Credit Transactions Act.
 - These policies and procedures will assist us in identifying situations that suggest identity theft, detecting when these situations occur, and responding to these situations appropriately, and are adopted with the understanding and support of the highest levels of practice administration, including the physician(s) and owner(s).
 - Our identity theft policies and procedures are subject to ongoing review and revision, and are part of our staff training and education process.
- b. This office is committed to ensuring the privacy of our patients' protected health information. We are committed to compliance with all privacy and security rules relating to the Health Insurance Portability and Accountability Act (HIPAA), along with other federal and state laws that are integral to matters of privacy, medical records, confidentiality of communications, and other topics addressed throughout this policy and procedure manual.

2. Covered Accounts for Identity Theft Compliance

Collection, utilization, and storage of personally identifiable information occur at all points of patient contact. Because most, if not all, of this information could be used to perpetrate identity theft, any records maintained by this office are considered "covered accounts" for the purpose of our identity theft prevention program. This includes:

- a. Personally identifying information such as a drivers license, address, or phone numbers used to manage patient flow, including appointment scheduling and registration;

- b. Personal health information such as medical history, prescriptions, allergies, or blood type used in the delivery of health care services; and
- c. Personal information such as insurance coverage, financial account data, Social Security numbers, and other patient information used by this office to seek payment for our services.

3. Red Flags for Identity Theft

The following scenarios should raise our level of concern regarding the possibility of identity theft patterns, practices, or activities. If any of these red flags occur, the staff member or physician involved will respond immediately to prevent/mitigate the threat of identity theft (see Section 4).

a. Appointment scheduling and patient registration:

- A patient is unable or unwilling to provide information requested during the appointment process. Examples include date of birth or address.
- The presented documentation appears to be forged or altered.
- A patient supplies identifying documentation (such as a drivers license) in which the physical description or photograph does not match his or her physical appearance.
- The presented documentation is inconsistent with other readily available documentation in the office records such as a patient signature from previous office encounters.
- There are discrepancies on patient documentation, such as different dates of birth or a Social Security number that already is associated with another patient in the practice.

b. Delivering patient care:

- Records indicate medical treatment that is inconsistent with a physical examination or medical history as reported by the patient.
- The patient indicates that the patient history documented in his or her medical record is not correct.
- Information in the medical record at the time of patient care is contradictory to your personal knowledge of the patient.
- The patient's description in the chart — such as age, height, or scars — is not consistent with the patient presenting for care.

c. Patient billing:

- The patient or an insurance company reports that coverage for a legitimate service is denied because insurance benefits have been depleted or that the patient's lifetime cap on benefits has been reached.
- The patient notified the office of an address change, yet the address presented by the patient does not match that address or the address recorded for previous patient visits.
- Mail sent to the patient is repeatedly returned as undeliverable, although the patient continues to be active with the practice.
- A patient disputes a bill, claiming he or she may be a victim of identity theft.

d. Answering patient inquiries:

- The patient receives a bill or receipt for services provided to another individual.
 - The patient receives a bill, notice of insurance benefits, or collection notice for health services never received, or from a health care provider that he or she never patronized.
 - The patient has a complaint or question about information added to a credit report by a health care provider or insurer.
 - A patient calls with an address change that does not appear legitimate, e.g., it is for a commercial establishment, vacant property, or a jail.
 - A patient notifies this office that he or she is not receiving explanations of benefits (EOBs), although they have been sent to the last address on file for the patient.
- e. Inquiries from a third party:
- We receive a notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.
 - The U.S. Postal Service notifies this office that the address given for the patient is not accurate, e.g., the address is for a commercial establishment, vacant property, or a jail.
 - The Social Security Administration notifies this office that the Social Security number provided by the patient is listed on the Social Security Administration's Death Master File.
 - Law enforcement notifies this office that there has been an identity theft.
 - Any other physician office, a hospital, or other provider caring for a patient notifies this office that there has been an identity theft.
- f. Access or use of credit reports on patients:
- This office receives an alert, notification, or other warning from a patient.
 - This office receives an alert, notification, or other warning from a report agency or a service provider, such as a fraud detection service.
 - A fraud or active duty alert is included with a consumer report obtained by this office.
 - A consumer reporting agency provides this office a notice of a credit freeze in response to a request for a consumer report or a notice of an address discrepancy.
 - A consumer report obtained by this office indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a patient, e.g., a recent and significant increase in the volume of inquiries; an unusual number of recently established credit relationships; or a material change in the use of credit, especially recently established credit relationships.
 - This office discovers that a patient's account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

4. Responding to Red Flags for Identity Theft

- a. The following actions should be taken if any of the red flag scenarios listed in Section 3 occurs:
- The patient in question will be notified to see if any discrepancy can be explained or clarified.
 - If the matter is not a simple misunderstanding, notify the management team, including the treating physician(s).
 - Any patient who appears to be a victim of identity theft will be notified by mail or properly-

documented telephone call. Documentation of any communication will be retained in the office records.

- Any patient who appears to be a victim of identity theft, whether from internal or external sources, will be advised to contact law enforcement and consider having a fraud alert placed on his or her credit file.
 - Law enforcement will be notified as deemed appropriate by management whenever this office has evidence of identity theft. This includes when the perpetrator of the crime is one of our own staff or physician(s).
 - In any case involving identity theft, we will suspend any collection attempts on the account until it can be clarified if the person receiving the treatment is the person being billed.
 - If it appears a patient has fraudulently received care from this office, we will aggressively pursue, to the extent possible, any resulting debt through our attorney, collection agency, or law enforcement.
 - This office will delay any notice to any person or entity if requested to do so, with proper documentation, by law enforcement, as in the case of a criminal investigation, or by a government entity such as in the case of national security.
- b. In addition to the above, the following actions will be taken if it appears the identity theft crime appears to be internal to this office:
- Any patient who appears to be a victim of identity theft by a person **inside** this office will be given the following information: 1) description of the incident in general terms; 2) the type of identifying information that was subject to the theft; 3) Steps this office has taken to protect the patient's information from further unauthorized access or use; and 4) the name and number of the privacy officer, billing supervisor, office manager, or any other person to whom the patient may wish to speak about the incident.
 - All passwords, PINs, locks, and other access to patient information (digital and on paper) will be changed as necessary to prevent further theft.
 - Any employee causing suspicion will be disciplined and suspended or terminated according to the employee policies and procedures of this office.
- c. In addition to all of the above, the following action will be taken in cases where it is suspected that a patient's **medical** identity has been stolen:
- The patient and/or his or her legal representative will be notified immediately.
 - The patient or his or her legal representative will be asked to review any of the patient's medical records in the possession of this office.
 - Any other physician, hospital, or provider involved with the patient's care will be notified that the patient's medical record may contain inaccurate information that could result in a patient safety issue.
 - Our liability carrier will be notified that we have become aware that we may have been treating a patient based on inaccurate information.
 - A "Jane Doe" or "John Doe" chart will be created (see below).
- d. Creation of a "Jane Doe" or "John Doe" chart:
- When this office has confirmed that medical identity theft has occurred, all inaccurate information will be removed from the patient's chart.

- Any purged, inaccurate information will be placed in a new, separate chart that will be filed as a “Jane Doe” or “John Doe” if the identity of the thief is not known. Otherwise the chart will be labeled with the correct patient name.
 - The new chart, regardless of whether the thief is known, will be cross-referenced with the theft victim’s original chart for accuracy and audit purposes.
- e. Any time a red flag situation occurs, the HIPAA privacy officer and the HIPAA security officer will be notified so that they may investigate whether a violation of a patient’s HIPAA rights also has occurred (see HIPAA Privacy Rule Policies and Procedures and HIPAA Security Rule Policies and Procedures).

5. Identity Theft Compliance: Plan Update and Staff Training

The policies and procedures comprising our plan to identify, prevent, and/or mitigate identity theft will be reviewed and updated on an ongoing basis.

- a. Updates will occur upon receipt of the following:
- Notices from law enforcement or government agencies;
 - Suggestions from consultants, educational programs, or process improvement activities;
 - Requirements of our liability insurance carrier(s); or
 - Requirements under new or revised state or federal laws.
- b. Staff training will include:
- New-employee orientation,
 - Ongoing staff training as requested by management and/or staff,
 - Training in response to any red flag occurrence in this office,
 - Training in coordination with ongoing HIPAA-related education (see HIPAA policies and procedures).

6. Identity Theft Compliance by Service Providers

Any third party granted access to our patients’ private information (medical, financial, or personal identifiers) must take steps to protect our patients from red flag events. Accordingly, all business associate agreements or other contractual agreements with third parties will include language binding third parties to appropriate measures to protect our patients from identity theft (see Business Associates Policies and Procedures).

7. Identity Theft Compliance: Approval at the Highest Level of Authority

All of the policies and procedures regarding these red flag rules are adopted with the full understanding and support of all levels of this office’s administration, including any physician(s) and any owner(s) of this practice.

- a. The high level of importance placed on the red flag policies and procedures is consistent with the high level of importance placed on all of the policies and procedures regarding patient privacy, the control over access to medical records, protections of patients’ protected health information, and other measures this office takes to comply with all of the various components of HIPAA.

- b. Any incidence of a red flag occurrence and/or any occurrence of a breach of any policy or procedure regarding patient privacy will be reported immediately to all levels of management of this office, including any physician(s) and/or owner(s).
- c. If no breaches occur, the effectiveness of this office's policies and procedures regarding the protection of patient privacy and protection from identity theft will be evaluated at least annually.
- d. This office understands that the importance of all of these policies can be demonstrated by the adoption of policies and procedures through an entity's board of directors. As we do not have a board of directors at this point in time, a similar level of approval is demonstrated by the adoption of all of these policies and procedures with the full understanding and support of all levels of administration of this practice, including any physician(s) and owner(s) of this practice.

Notice to Those Who Utilize These Policies and Procedures

The information, opinions, and supplemental materials presented should not be used or referred to as primary legal sources, nor construed as establishing medical standards of care for the purposes of litigation, including expert testimony. The standard of care is dependent upon the particular facts and circumstances of each individual case and no generalization can be made that would apply to all cases.

Further, information presented should be used as a resource, selected and adapted with the advice of your attorney. This information is distributed with the understanding that the Texas Medical Association is not engaged in rendering legal or other professional services.

- These policies and procedures are specific to the Red Flag Rules required by the Fair and Accurate Credit Transactions Act of 2003 and do not reflect HIPAA compliance practices.
- In order to fully comply with the Red Flag Rules, a practice will need both identity theft policies and procedures and HIPAA policies and procedures to dictate privacy and security practices generally.
- Also of importance: The Red Flag Rules are not a “one-size-fits-all” standard. In fact, they state that an identity theft prevention program must be “appropriate to the size and complexity of the [office] and the nature and scope of its activities.”
- These policies and procedures are based on a physician practice that represents the majority of TMA members — a small office with five or fewer physicians and other providers, and no dedicated information technology (IT) department. Larger practices may need to revise these policies and procedures — although they are a good place for these practices to start — to reflect the scope of their activities. In particular, practices with dedicated IT personnel should coordinate the development of their red flag rules with those people/departments.