



Bay Area Orthopedic Surgery and Sports Medicine

100 Hospital Drive
Suite 303
Vallejo, CA 94589
Ph: 707-645-7210 Fax: 707-645-7249

Identity Theft Prevention Program Effective 1/1/2010

I. Purpose

The Identity Theft Prevention Program was developed by Bay Area Orthopedics in order to comply with the Federal Trade Commission's Identity Theft Prevention Red Flags Rule (16 CFR § 681.2).

The purposes of the Program are to:

1. Identify relevant Red Flags based on the risk factors of the medical practice;
2. Institute policies and procedures to detect Red Flags;
3. Identify steps the Practice will take to prevent and mitigate Identity Theft;
4. Identify appropriate responses to Red Flags, should they occur; and
5. Create a system of administrative oversight and periodic updating of the Program.

II. Definitions

For purposes of the Program, the following terms are defined as follows:

1. "Covered Account" means (i) an account used primarily for personal, family or household purposes, and that involves or is designed to permit multiple payments or transactions, or (ii) any other account for which there is a reasonably foreseeable risk to patients or the safety and soundness of the Practice from identity theft. The Practice has identified the following types of accounts as Covered Accounts:
 - a. Accounts to which insurance companies are billed;
 - b. Accounts for which payment plans have been approved; and
 - c. Accounts that a patient pays with a personal check or credit card.
2. "Identity Theft" means a fraud committed or attempted using the identifying information of another person without his or her permission.

3. “Medical Identity Theft” means identity theft for the purpose of obtaining medical services.
4. “Red Flag” is a pattern, practice or specific activity that indicates the possible occurrence of identity theft.

III. Identification of Red Flags

The Practice has identified relevant Red Flags to include:

1. The presentation of documents under the following suspicious circumstances:
 - a. Documents provided for identification and that appear to have been altered or forged;
 - b. The photograph or physical description on the identification is not consistent with the appearance of the patient presenting the identification;
 - c. Other information on the identification is not consistent with information provided by the new patient or patient presenting the identification; and
 - d. Other information on the identification is not consistent with readily accessible information that is in the patient’s chart or practice management system.
2. The presentation of suspicious personal identifying information such as the following:
 - a. The Social Security Number (“SSN”) provided is the same as that submitted by another patient;
 - b. The patient has an insurance number but does not produce an insurance card; and
 - c. The patient has same name and date of birth as another patient.
3. The unusual use of, or other suspicious activity related to, a covered account:
 - a. Medical record indicates a medical treatment that is inconsistent with medical history as reported by the patient or physical examination (*e.g.*, inconsistent height, weight, blood type, medical conditions, *etc.*); and
 - b. Mail sent to the patient is returned repeatedly as undeliverable although patient continues to receive medical services.

4. Notice from patients, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts held by the Practice, such as the following:
 - a. Complaint/inquiry from an individual based on the receipt of a bill for another individual, a bill for a service that the individual denies receiving, an Explanation of Benefits (EOB) for a service that the individual denies receiving, a charge on an individual's credit card for service that the individual denies receiving, or a notice from a collection agency for a service that the individual denies receiving; and
 - b. Notice from a patient, a victim of identity theft, law enforcement authorities or any other person that the Practice has opened a fraudulent account for a person engaged in identity theft.

IV. Detection of Red Flags

The Practice will take the following steps to obtain and verify the identity of the person in question as follows:

1. New Patients
 - a. Require all new patients to submit a valid photo identification issued by a local, state or federal government agency for the visit (*e.g.*, driver's license, passport, military ID, *etc.*) and include in each patient's file a scanned/copy of the ID as submitted:
 - i. In the case where the new patient is a minor, photo identification of the patient's responsible party will be obtained; and
 - ii. In the case where a new patient does not have a valid photo ID, two forms of non-photo ID, one of which is issued by a state or federal agency, will be obtained (*e.g.*, birth certificate, Social Security card, voters registration card, lawful permanent residence card or "Green Card," *etc.*);
 - b. For new patients with insurance, verify information with their identified insurance company;
 - c. For new patients paying by credit card, confirm that photo identification and name on credit card is the same;

- d. For new patients paying by personal check, ensure photo identification and name on personal check is the same;
- e. For new patients on a payment plan, obtain two forms of identification; and
- f. [If practice performs a credit check for payment plans, mention that here]

2. Existing Patients

- a. Verify identification of patients at each visit or before giving out any personal information by matching photo identification to the one on record [this procedure will vary depending on practice. Practices in a tight knit community may be able to verify on sight if staff personally know the patients. Practices in urban areas may need to check photo identification for each visit.]; and
- b. Verify validity of requests for changes of billing addresses.

3. Emergency Care

In the event of emergency care, NO DELAY. The process of confirming either a new or existing patient's identity must never delay the provision of appropriate medical care for emergency medical situations.

4. Responding to Questions

When asked the reason for the identifying procedures, explain the procedures are for *patient protection* to prevent identity theft. This is common procedure when paying by credit card, cashing a check, checking into a hotel, boarding an airplane, *etc.*

5. Refusal to Provide or Lack of Identification

No one should be refused care because they do not have valid identification with them. This is distinguished from patients who present fraudulent identification. Depending on the situation, ask for a cash payment for today's visit, reschedule the visit after consulting with a nurse or physician (sick patient versus a routine check-up), or ask patient to bring appropriate identification to their next visit. Flag the patient's chart and/or practice management system to verify at next visit.

V. Prevent and Mitigate Identity Theft

In order to prevent and mitigate identity theft, the Practice will take the appropriate steps in response to any Red Flags that are identified:

1. Stop the billing process: do not bill an insurance company, accept a personal check or credit card, or set a patient up for a payment plan, but rather require the patient to provide satisfactory information to verify identity;
2. Investigate the complaint or situation as appropriate; and
3. Investigate allegations of identity theft, including making a determination of whether the billing or payment was made fraudulently.

VI. Protecting Patient Financial Information

The Practice will take reasonable measures to protect patient financial information that could be used fraudulently to commit identity theft by staff or other individuals with physical access within the Practice. Patient financial information includes demographics, credit card and check information, SSNs, and insurance information. The Practice will also undertake the follow activities:

1. Conduct full background and credit checks prior to hiring employees;
2. Require all personnel to sign confidentiality agreements;
3. Maintain patient credit card information for payment plans or deferred payments in a locked safe with access limited only to staff with a need for the information (and once a payment plan is satisfied, all relevant credit card information will be shredded or otherwise destroyed);
4. Shred or otherwise destroy all patient credit card information received by mail for specific payments once a receipt has been issued to the patient;
5. Implement a password-based security system to protect the practice management system from unauthorized access;
6. Restrict access to patient financial information in the practice management system to authorized staff [if available by system];
7. Prohibit the sharing of passwords by Practice personnel, and mandate the changing of all passwords every 30 – 45 days;
8. Upon the termination of the employment of any Practice personnel, his or her access (if any) to Practice computer systems and programs are to be immediately deactivated;
9. Paper documents containing patient financial and/or practice information are to be shredded before disposing of them.

10. Reasonable measures to protect patients' SSNs and copies of drivers licenses are to be implemented;
11. Disaster recovery plans are to be implemented and then re-evaluated on a periodic basis;
12. The Practice shall maintain an indemnity bond covering instances of identity theft;
13. Practice personnel will be prohibited from transferring or otherwise sending confidential patient or practice information via electronic mail;
14. Practice management shall conduct periodic audits to determine if staff have accessed or attempted to access patient accounts for which they do not have responsibility; and
15. The Practice has and adheres to the privacy policies outlined by The Health Insurance Portability and Accountability Act ("HIPAA").

VI. Responses to Red Flags

In the event that a Red Flag is identified, the Practice will take the following responses based on individual circumstances, as appropriate:

1. Notify the individual whose identity was compromised;
2. Cease collection efforts on the account;
3. Notify law enforcement;
4. Notify insurance carrier, Medicare or Medicaid;
5. In the event of actual fraud, offer affected individual free credit monitoring service for one year;
6. Flag the affected patient's chart for an alert that a Red Flag exists for this patient; and
7. Determine that no response is warranted under the particular circumstances.

VII. Program Administration

The Office Manager, is responsible for developing, implementing and updating the Program as well as providing training for all staff who have a role in implementing the Program.

Oversight of service provider arrangements: Whenever the Practice engages a service provider to perform an activity in connection with one or more covered accounts, the Practice requires the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VIII. Updating the Program

The Office Manager is responsible for reviewing and updating the Program periodically, as necessary, to reflect changes in risks to patients from identity theft, based on factors such as:

1. The experiences of the Practice 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 Practice offers or maintains;
and
5. Changes in the business arrangements of the Practice, including mergers, acquisitions, alliances and joint ventures.