FOX VALLEY ORTHOPEDICS

Identity Compliance Program

I. ADOPTION OF WRITTEN PROGRAM ("Program")

Fox Valley Orthopedics (the "Practice") adopts this written program to assist in identifying sensitive information, as well as identifying, detecting and mitigating risks of identity theft affecting the patients of the Practice. This program is intended to comply with requirements of 16 C.F.R. Section 681.2 (2008) (the "FTC Regulations") and terms not otherwise defined herein shall have the same meaning as in the FTC Regulations.

II. SENSITIVE INFORMATION

Sensitive information is information which, if lost or misused, could prove damaging to employees, physicians, patients and the Practice. Sensitive information includes the following items whether stored in electronic or printed format:

A. Personal Information – including but not limited to:
   1. Credit Card Information, including any of the following:
      a. Credit card number (in part or whole)
      b. Credit card expiration date
      c. Cardholder name
      d. Cardholder address

   2. Tax Identification Numbers, including:
      a. Social security number
      b. Social insurance number
      c. Business identification number
      d. Employer identification numbers

   3. Payroll information, including:
      a. Paychecks
      b. Pay stubs
      c. Pay rates

   4. Flexible Spending Requests and associated paperwork

   5. Medical Information for any Employees or Customers, including:
      a. Doctor names and claims
      b. Insurance claims
      c. Prescriptions
      d. Any related personal medical information

   6. Other Personal Information belonging to Patients, Physicians, Employees and Contractors, examples of which include:
      a. Date of birth
      b. Address

c. Phone numbers
d. Maiden name
e. Names
f. Chart number
g. Drivers license information
h. Bank account information

B. Corporate Information – including but not limited to:
   1. Company, employee, physician, patient, vendor, supplier confidential, proprietary information or trade secrets.

   2. Proprietary and/or confidential information, among other things, includes: business methods, marketing and other Practice strategy, negotiated vendor pricing, computer codes, passwords, forms, information about or received from the Practice's current and former patients or any other non-public information. Proprietary and/or confidential information also includes the name and identity of any patient or vendor and the specifics of any relationship between and among them and the Practice.

C. Any document marked "Confidential," "Sensitive," "Proprietary," or any document similarly labeled.

D. Practice personnel are encouraged to use common sense judgment in securing Practice Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor/manager.

III. IDENTIFYING RELEVANT RED FLAGS

The Practice has considered various factors in identifying relevant red flags for possible identity theft affecting covered accounts of the Practice, including without limitation the following factors: the types of covered accounts it offers or maintains; the methods it provides to open its covered accounts; the methods it provides to access its covered accounts; and its previous experiences with identity theft.

Based on this analysis, the Practice has identified the following relevant red flags:

A. A complaint or question from a patient based on the patient's receipt of:
   1. a bill for another individual;
   2. a bill for a product or service that the patient denies receiving;
   3. a bill from a healthcare provider that the patient never patronized; or
   4. a notice of insurance benefits (or Explanation of Benefits) for health services never received.

B. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.

C. A complaint or question from a patient about the receipt of a collection notice from a bill collector that the patient or insured is disputing services were rendered.

D. A patient or insurance company report that coverage for legitimate healthcare services is denied because insurance benefits have been depleted or a lifetime cap has been reached.

E. A complaint or question from a patient about information added to a credit report by a healthcare provider or outside collection agency.

F. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

G. A patient who presents suspicious documentation of insurance and/or identity.

H. A patient who presents documentation of insurance and/or identity with home address information that is different from that found in other sources.

I. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance and/or identity.

J. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

IV. DETECTING RED FLAGS

The Practice has adopted the following policies and procedures that aid the Practice in detecting red flags for identity theft:

A. For a patient opening a new covered account: obtaining appropriate identifying and insurance information;

B. For a returning patient: obtaining and/or updating appropriate identifying and insurance information;

C. Verifying validity of changes to existing covered accounts, such as address.

D. Listening for verbal cues of identity that differ from written sources, such as driver's license or insurance card.

E. Dissemination of this written Program to all Practice employees having patient interaction.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In determining an appropriate response to a red flag or other threat of identity theft, the Practice will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a patient's account records, or notice that a patient has become aware of someone fraudulently claiming to obtain medical services in the name of the patient.

Appropriate responses may include the following:

A. Monitoring a covered account for evidence of identity theft;

B. Contacting the patient;

C. Contacting the insurance carrier;

D. Changing any passwords, security codes, or other security devices that permit access to a covered account;

E. Reopening a covered account with a new account number;

F. Not opening a new covered account;

G. Closing an existing covered account;

H. Not attempting to collect on a covered account or not selling a covered account to a debt collector;

I. Notifying law enforcement; or

J. Determining that no response is warranted under the particular circumstances.

VI. UPDATING THE PROGRAM

The Practice will evaluate the Program on an annual basis and will update the Program as necessary to reflect changes in risks to patients or to the Practice from identity theft, based on factors such as:

A. The experiences of the Practice with identity theft;

B. Changes in methods of identity theft;

C. Changes in methods to detect, prevent and mitigate identity theft;

D. Changes in the types of accounts that the Practice offers or maintains; and

E. Changes in the business arrangements of the Practice, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VII. PROGRAM ADMINISTRATION

The Chief Compliance Officer of the Practice shall assume primary administration of the Program, subject to oversight by the Board of Directors of the Practice. The Chief Compliance Officer shall report to the Board of Directors of the Practice, at least annually, on compliance by the Practice with the Program. The report shall address material matters related to the Program and evaluate issues such as:

A. The effectiveness of the policies and procedures of the Practice in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

B. Any third party service provider arrangements relevant to covered accounts;

C. Significant incidents involving identity theft and management's response; and

D. Recommendations for material changes to the Program.

Any modification or amendment to the Program shall be adopted by the Board of Directors of the Practice.

This Program has been adopted by the Board of Directors of the Practice effective as of May 1, 2009.