EMMITSBURG OSTEOPATHIC PRIMARY CARE CENTER, INC.

Identity Theft Prevention Program

Effective beginning May 1, 2009

I. PROGRAM ADOPTION

Emmitsburg Osteopathic Primary Care Center, Inc. ("Physician Practice") has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rules ("Red Flag Rules"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the Physician Practice's Board of Directors. After consideration of the size and complexity of the Physician Practice's operations and the nature and scope of the Physician Practice's activities, the Board of Directors determined that this Program was appropriate for the Physician Practice, and therefore approved this Program on April 21, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rules

Under the Red Flag Rules, every creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The FTC has taken the position that a Physician Practice may be a creditor subject to the requirements of the Red Flag Rules. Each Program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing patient accounts 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 patients.

B. Red Flags Rule definitions used in this Program

The Red Flags Rules define "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

"Identifying information" is defined under the Red Flag Rules as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number,

government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Physician Practice considers the types of patient accounts that it maintains, the methods it provides to open the accounts, the methods it provides to access the patient accounts, and its previous experiences with Identity Theft. The Physician Practice identifies the following Red Flags, in each of the listed categories:

A. Notifications and Warnings From Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a patient;
3. Notice or report from a credit agency of an active duty alert for a patient; and
4. Indication from a credit report of activity that is inconsistent with a patient's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a patient's photograph or physical description is not consistent with the patient presenting the document; and
3. Other document with information that is not consistent with existing patient information (such as if a patient's signature on a check appears forged).

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the patient provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other documents that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another patient;
6. An address or phone number presented that is the same as that of another person;
7. A person's identifying information is not consistent with the information that is on file for the patient.

D. Suspicious Account Activity or Unusual Use of Patient Account

Red Flags

1. Mail sent to a patient is repeatedly returned as undeliverable;
2. Notice to the Physician Practice that a patient is not receiving mail sent by the Physician Practice;
3. Breach in the Physician Practice's computer system security; and
4. Unauthorized access to or use of patient information.

E. Alerts from Others

Red Flags

1. Notice to the Physician Practice from a patient, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. New Patients

In order to detect any of the Red Flags identified above associated with a new patient, Physician Practice personnel will take the following steps to obtain and verify the identity of a new patient:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification; and
2. Verify the patient's identity (for instance, review a driver's license or other identification card);

B. Existing Patients

In order to detect any of the Red Flags identified above for an **existing patient**, Physician Practice personnel will take the following steps to monitor transactions:

Detect

1. Verify the identification of patients if they request information (in person, via telephone, via facsimile, via email); and
2. Verify the validity of requests to change billing addresses.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Physician Practice personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor the situation for evidence of Identity Theft;
2. Contact the patient;
3. Change any passwords or other security devices that permit access to accounts;
4. Notify the Program Administrator for determination of the appropriate step(s) to take;
5. Notify law enforcement; or
6. Determine that no response is warranted under the particular circumstances.

Protect patient identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Physician Practice patient records, the Physician Practice will take the following steps with respect to its internal operating procedures to protect patient identifying information:

1. Ensure that office computers are password protected and that computer screens lock after a set period of time;
2. Keep offices clear of papers containing patient information;
3. Ensure computer virus protection is up to date; and
4. Require and keep only the kinds of patient information that are necessary for Physician Practice purposes.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to patients and the soundness of the Physician Practice from Identity Theft. At least every year, the Program Administrator will consider the Physician Practice's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods and changes in the Physician Practice's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the Board of Directors with his or her recommended changes and the Board of Directors will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the

Practice Manager. The Practice Manager will be responsible for the Program administration, for ensuring appropriate training of Physician Practice staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Physician Practice staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements

In the event the Physician Practice engages a service provider to perform an activity in connection with one or more patients, the Physician Practice will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the Physician Practice's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Physician Practice's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Practice Manager, Physicians and those employees who need to know them for purposes of preventing Identity Theft. Only the Program's general red flag detection, implementation and prevention practices are listed in this document.

I HEREBY CERTIFY that the above Identity Theft Prevention Program was adopted on the 21 day of April, 2009, by the CEO, Bonita J. Krempel-Portier, D.O. of Emmitsburg Osteopathic Primary Care Center, Inc.

Bonita J. Krempel-Portier, D.O.

Bonita J. Krempel-Portier, D.O.
CEO

4/13/9

c:\mydocuments\RedFlagPolicy