

MEDICAL IDENTITY THEFT PREVENTION PROGRAM
(Condensed form)

Overview.

We are a health care provider who has been qualified by the Federal Trade Commission (FTC) as a Creditor because we maintain covered accounts (e.g.: patient accounts). Therefore, by law we are required to develop, implement, and monitor a working Identity Theft Prevention Program. This document defines our complete and LRA board-approved Identity Theft Prevention Program.

Definition.

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 victim's knowledge or consent to obtain medical services or goods, or when someone uses the person's identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims, as defined by the World Privacy Forum.

Purpose.

The purpose of our Program is to detect, prevent, and mitigate identity theft in connection with new and existing covered (patient) accounts. We believe that our Program is appropriate to the size and complexity of our position as a patient creditor and the nature and scope of our medical service activities.

Considerations.

Our Program takes these three (3) concepts into consideration:

1. The methods we provide to open our covered patient accounts,
2. The methods we provide to access our accounts, and
3. Our previous experience with identity theft.

Required Elements.

There are four (4) required elements of our Program; we include reasonable policies and procedures to:

1. Identify relevant Red Flags for the covered accounts that we maintain and incorporate those Red Flags into our Program,
2. Detect Red Flags that have been incorporated into our program,
3. Respond appropriately to any Red Flags that are detected, and
4. Update our program periodically to reflect changes in risks from identity theft to patients and to the safety and soundness of our Practice from identity theft.

Administration.

There are four (4) elements to the administration of our Program:

1. Written program approval from our managing Board of Directors,
2. Involve by our Board and designated senior management in the oversight, development, implementation, and administration of Our Program,

3. Train staff to effectively implement our Program, and
4. Exercise appropriate and effective oversight of service provider and third party business arrangements.

Business Associates.

We require our external business associates to possess and follow their own documented Identity Theft Prevention Program as well. Business Associates are external parties providing professional services to our Practice (e.g.: Collection Agencies, Billing Companies, Attorneys, and Consultants).

Protected Health Information (PHI).

Below is a list of 18 identifiers we consider to be protected health information, according to our interpretation of the HIPAA law of 1996:

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes.
3. Dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

Red Flags.

The following is a list of healthcare-related Red Flags which our Program monitors:

- A complaint or question from a patient based on the patient's receipt of:
 - a bill for another individual
 - a bill for a product or service that the patient denies receiving
 - a bill from a health care provider that the patient never patronized, or

- an Explanation of Benefits or other notice for health services never received.

An unexpected bill or notice of benefits can be one way that a patient can learn that she has been a victim of medical identity theft. Explanations of Benefits (EOBs) are potentially important tools for patients and providers. For example, hotline information to report possible fraudulent or suspicious activity can be included on an EOB. Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient. In particular, records that show substantial discrepancies in age, race, and other physical descriptions may be evidence of medical identity theft. The World Privacy Forum Medical Identity Theft report (page 33) illustrates how an incorrect blood type was evidence that the patient was a victim of medical identity theft.

- A complaint or question from a patient about the receipt of a collection notice from a bill collector.

The World Privacy Forum Medical Identity Theft report (page 31) shows how a collection notice can be one way that a patient can learn that she has been a victim of medical identity theft.

- A patient or insurance company report that coverage for legitimate hospital stays are being denied because insurance benefits have been depleted, or that a lifetime cap has already been reached.

The World Privacy Forum Medical Identity Theft report (page 34) illustrates how members of a family can be victimized by “looping”, where a thief uses one family member’s benefits and then turns to the next family member when the first victim’s benefits have run out.

- A complaint or question from a patient about information added to a credit report by a health care provider or insurer.

The World Privacy Forum Medical Identity Theft report (page 32) shows how an entry in a credit report can be one way that a patient can learn that she has been a victim of medical identity theft.

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

Although financial identity theft differs significantly from medical identity theft, a victim of financial identity theft may be more likely to also be a victim of medical identity theft. Victims of financial identity theft may have filed police reports about their case, and these need to be taken into account.

- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.

A medical identity thief may succeed by obtaining the medical insurance number and other information about the victim. The absence of an actual insurance card is evidence suggesting that the person being treated may not be the actual insured.

Note: This particular Red Flag has to be applied with caution because there are other reasons a patient may not have her insurance card.

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

Not all forms of medical identity theft are the result of an individual thief presenting for treatment. The World Privacy Forum Medical Identity Theft report (page 33) illustrates how fraudulent billing by a physician can result in false information in a health record that may affect the treatment of patients. In some cases, clerks, nurses

(Condensed form) Identity Theft Prevention Program of Limestone Radiology Associates, P.C., DBA: Valley Imaging Center

and other hospital employees have exploited their legitimate access to health files to use the information for personal or financial benefit.

Red Flag / HIPAA Committee.

Our Practice has identified a three (3) member committee with the responsibility to meet on a monthly basis to review issues and amend our Program as necessary.

Committee Responsibilities.

Our committee will meet monthly to review and amend Program policies, procedures, and Red Flag alerts. We will review new regulations relevant to the protection of patient information. We will conduct periodic education for committee member, employees and potentially patients. Upon identification of a security breach or Red Flag alert, we will meet to review and resolve any compliance issues relating to a patient's Protected Health Information (PHI) or Medical Identity Theft. We will execute notification and documentation procedures to senior management and the patient relevant to the security breach or identity theft.