



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

Scope:

This policy applies to all Essent facilities.

Purpose:

The purpose of this policy is to establish guidelines for the detection and prevention of medical identity theft, and mitigation of any harm caused by medical identity theft.

Policy:

Essent Healthcare's Red Flag Identity Theft Prevention Program, in accordance with the Federal Trade Commission's Fair and Accurate Credit Transactions (FACT) Act of 2003, is established to implement written policies and procedures for detecting or mitigating identity theft covering both new and existing covered patient accounts. It is the policy of Essent to:

- Identify relevant patterns, practices, and specific activities that signal possible identity theft and incorporate "red-flags" into its identity theft program.
- Detect and report "red-flags" that have been incorporated into the program.
- Respond appropriately to any "red-flags" that are detected.
- Update the program periodically to reflect changes in risks.
- Train staff as necessary to effectively implement the program.
- Exercise appropriate and effective oversight of the program.
- Report all known or suspected instances of identity theft to the appropriate authorities and, if applicable, to any insurance plans connected to the incident.
- Mitigate any harm that may be caused by any potential occurrences of identity theft.

Definitions:

***"Medical identity theft"** occurs when a thief uses someone's personal information, such as health insurance information, without the individual's consent to obtain medical goods or services, or to make false claims for medical goods or services. Unlike purely financial forms of identity theft, medical identity theft may also harm its victims by creating false entries in their medical records. Victims of medical identity theft may receive the wrong treatments, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage due to the*



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

presence of diseases in their health record that do not belong to them.

*A **“Red Flag”** is a pattern, practice, or specific activity that indicates the possible existence of identity theft such as alerts, notifications, or other warnings received from consumer reporting agencies; the presentation of suspicious documents; the presentation of suspicious personal identifying information such as a suspicious address change; and/or notice from customers, victims of identity theft, or law enforcement regarding possible identity theft in connection with covered accounts.*

*A **“covered account”** is a continuing relationship with a creditor to obtain a service and includes deferred payments for services, or an account primarily for personal, family, and household purposes that involves or is designed to permit multiple payments or transactions; and/or any other account for which there is a reasonably foreseeable risk to customers, or the safety and soundness of the creditor, from identity theft, including financial, operational, compliance, reputation, or litigation risks.*

Background:

Medical identity theft is a crime that can cause great harm to its victims. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims’ medical and financial lives for years. Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information – without the person’s knowledge to make false claims for medical goods or services. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name.

Victims of medical identity theft may experience the now-familiar consequences of financially oriented forms of identity theft. These can include the loss of credit, harassment by debt collectors, and inability to find employment. For example: Recently, a Colorado man whose Social Security Number, name, and address was stolen, found out he was a victim of medical identity theft when a bill collector wrote to demand the \$44,000 he owed to a hospital ... for a surgery he never had. The victim did not have insurance, and had to go through a lengthy procedure to clear his name, a process that is ongoing after more than two years.

But unlike purely financial forms of identity theft, medical identity theft may also harm its victims by creating false entries in their health records at hospitals, doctors' offices, pharmacies, and insurance



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

companies. Sometimes the changes are put in files intentionally; sometimes the changes are secondary consequences of the theft. The changes made to victims' medical files and histories can remain for years, and may not ever be corrected or even discovered.

Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them. It is nightmarish that patients' medical records may include information about individuals who have stolen their identities for the purposes of using the victims' insurance or for dodging medical bills. However, evidence exists that this is already occurring.

Medical identity theft can be difficult to uncover. It is typically well-hidden in large electronic payment systems and in widely dispersed databases and medical files. Medical identity theft does not always reveal itself through traditional financial avenues. Individuals who regularly check their credit reports, for example, may see no indication on the credit report that the problem exists, even if it is a significant one.

The people who commit medical identity theft can be sophisticated professionals who are adept at making sure victims do not detect the crime -- ever. Victims may only discover it many years later through an unhappy circumstance such as the discovery of an incorrect blood type on a medical chart, or the loss of a job opportunity after a background check reveals one or more diagnoses and diseases that didn't belong to them.

Because of the difficulty of detection, the potential exists for this crime to be happening substantially more frequently than anyone has documented to date. In response to the increase in the number of reported cases of medical identity theft, Essent is implementing a comprehensive program designed to detect and prevent medical identity theft as outlined below.

Procedure:

During the registration process, patients must be asked for picture identification along with their insurance card. The photo ID should be viewed and/or copied/scanned and filed in the same manner



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

as the insurance card as verification of the identity of the patient prior to providing services or billing insurance. In cases where patients are pre-registered via telephone, the patient should be instructed to bring a picture ID to the hospital along with their insurance card. If pre-registered patients present directly to the service departments, the service departments are responsible for viewing and/or copying the photo ID. The type of photo ID provided is to be denoted in the Meditech admission CDS screen and/or denoted manually on the facesheet.

Special Treatment of Emergency Department Patients - Essent facilities should request picture ID in addition to their normal registration process in the emergency department, however, the medical screening exam should never be delayed in order to collect insurance information or obtain ID. In emergent cases where patients are seen immediately upon arrival at the ED, identification may be obtained after the screening exam and any necessary treatments have been completed. This would be consistent with the existing registration process for emergent cases whereby insurance information is obtained and registration is completed after the patient has been stabilized.

Identification of Red-Flags

A “red-flag” is a pattern, practice, or specific activity that indicates the possible existence if identity theft. Below is a list of potential red-flags that all Essent employees should be on the lookout for. Should any of the red-flags listed below be identified by any Essent employee, it must be reported to the department supervisor or the compliance officer immediately for investigation.

1. Suspicious Documents:

- a. Documents provided for identification 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/customer presenting the identification
- c. Other information on the identification is not consistent with information provided by the person presenting the identification (i.e. address or phone number).

2. Suspicious Identifying Information:

- a. Personal identifying information provided is inconsistent when compared to existing Meditech data sources:
 - The name and/or address does not match
 - The phone number does not match



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

- The social security number does not match
- The date of birth does not match
- b. The social security number provided is the same as that submitted by others persons or on other accounts.
- c. The address or telephone number provided is the same or similar to the address or telephone number submitted by an unusually large number of other patients.
- d. The person registering for services fails to provide all required identifying information.
- e. Personal identifying information submitted is inconsistent with personal identifying information that is already on file.

3. Suspicious Activities Related to Patient Accounts:

- a. First statement mailed to the patient is returned as undeliverable by the postal carrier after which the staff is unable to locate a “good” address for the customer.
- b. The facility is notified by a patient/customer of unauthorized charges or transactions in connection with their account.
- c. The facility is notified that one of its patients has been the victim of identity theft.

4. Other Red Flags:

- a. 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 individual denies receiving
 - A bill from a health care provider that the patient never patronized
 - An Explanation of Benefits (EOB) or other notice for health services never received
- b. Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient. For example, records that show discrepancies in age, race, or other physical descriptions may be evidence of medical identity theft.
- c. A complaint or question from a patient about the receipt of a collection notice from a bill collector.
- d. A patient or insurance company report that coverage for a legitimate hospital stay is being denied because insurance benefits have been depleted or that a lifetime cap has



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

been reached.

- e. A complaint or question from a patient about information added to a credit report by a health care provider or insurer.
- 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 has an insurance number but never produces an insurance card or other physical documentation of insurance.
- h. A notice or inquiry from an insurance fraud investigator for a private insurance company or law enforcement agency.

Prevention and Mitigation of Medical Identity Theft

Upon receipt of notice of a fed-flag, the compliance officer shall conduct an investigation to determine if identity theft has occurred. Should an instance of identity theft be identified, the compliance officer, in conjunction with the affected facility, shall take one or more of the following actions:

1. Notify local law enforcement;
2. Notify any payer involved in the identity theft;
3. Monitor the account of the customer whose identity has been compromised for future potential fraudulent activity;
4. Review the medical record of the individual whose identity has been compromised for any suspicious activity or entries that do not correlate to past treatment experiences;
5. Flag the medical record of the individual whose identity has been compromised to alert future caregivers and to prevent the possibility of another person's information being recorded in the victim's medical file.

References:

The World Privacy Forum Suggestions for Health Care Providers 9/24/08
The World Privacy Forum Medical Identity Theft Report 5/3/06



ESSENT HEALTHCARE, INC.

Section: Corporate Compliance	Effective Date: 03/31/09
Subject: Medical Identity Theft	Revision Date: 10/21/09
Policy #: CC-6	Review Date: 10/21/09
Responsible Party: Corporate Compliance Officer	Revision #: 3

Federal Trade Commission "FTC Business Alert" June 2008
Federal Register Friday, November 9, 2007