Medical Identity Theft Prevention Policy – SAMPLE

Subject: Medical Identity Theft Prevention Policy
Number: 
Effective date: 
Supersedes SPP: 
Approved by:
(Signature) Date

Distribution: 

I. STATEMENT OF PURPOSE
To define “medical identity theft” and outline various measures to prevent, identify and mitigate medical identity theft.

II. STATEMENT OF POLICY
[Insert name of hospital/provider here] is committed to protecting patient identification and health insurance information from theft and fraudulent use. All employees, medical staff members and affiliates are responsible for reporting actual and suspected patient medical identity theft and threats to the security of related information.

III. PROCEDURE
A. Definitions:
• Medical Identity Theft: According to the World Privacy Forum: 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 or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods.¹
• Covered Account: Any account that [insert name of hospital/provider here] offers or maintains, primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions, including one or more deferred payments, or any other account of [insert name of hospital/provider here] for which there is a reasonably foreseeable risk to customers or to the safety and soundness of [list name of hospital/provider here] from identity theft.² Covered accounts include, but are not limited to:
  o Non-emergency patient billing
  o Patient payment plan
  o [Insert other accounts that have deferred payments]
• Red Flag: The World Privacy Forum defines a Red Flag as, “a pattern, practice, or specific activity that could indicate identity theft.”³ Examples include:
  o 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,
Medical Identity Theft Prevention Policy – SAMPLE

- A bill from a healthcare provider that the patient never patronized, or
- A notice of insurance benefits (or Explanation of Benefits) for healthcare services never received.
  - Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient.
  - A complaint or question from a patient about receipt of a collection notice from a bill collector.
  - 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 been reached.
  - A complaint or question from a patient about information added to a credit report by a healthcare provider or insurer.
  - A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
  - A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
  - A notice or inquiry from an insurance fraud investigator for private insurance company or law enforcement agency.

- Notice of an Address Discrepancy: A notice sent by a credit bureau to a person or business that requested a credit report that there is a discrepancy in the consumer/patient’s address. NOTE: the notice of address discrepancy triggers an investigation and management under the Red Flags Rule.

B. General Information
1. The Federal Trade Commission’s Identity Theft Red Flags Rule requires creditors to develop and implement written identity theft protection programs. The [insert title of responsible individual] and the appropriate oversight committee are responsible for developing, implementing, administering and updating the program, upon approval by the governing body.
2. The [insert title of responsible individual] is responsible for the oversight of the Medical Identity Theft Protection Program (Program).
3. The [insert title of responsible individual] shall establish and coordinate a committee (Committee) for the Program. See Part F of this section regarding Committee duties.
4. Committee members may include, but are not limited to, representatives from the following departments:
   a. Compliance
   b. Medical records
   c. Billing
   d. Patient registration
   e. Medical staff office
   f. Information technology
   g. Patient complaints/management

This document is a work product of Coverys’ Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Updated: December 2018
h. Risk Management

C. Prevention of Medical Identity Theft

1. Employee Background Check Procedures:
   a. Background checks will be conducted on all new employees (refer to [insert title of policy] policy for details regarding employee background checks).

2. Patient Identification Procedures:
   a. Reasonable efforts will be implemented to verify the patient’s identity when new or existing patient account transactions occur.
   b. New Patient Accounts:
      i. Verify patient identification (e.g., name, date of birth, address, driver’s license, government issued picture identification, insurance card).
   c. Existing Patient Accounts:
      i. When applicable, verify patient identification (e.g., name, date of birth, address, driver’s license, government issued picture identification, insurance card).
      ii. Verify the validity of requests for change of billing address.
      iii. Verify patient identification prior to providing personal information.

3. Medical Record Security:
   a. All paper medical records and patient charts shall be maintained in a secured and/or designated area and/or under the complete control of an employee at all times. Please refer to [insert title of policy] policy for additional information.
   b. All computers will be password protected and locked when the operator is away from the computer. Please refer to [insert title of policy] policy for additional IT security information and requirements.
   c. All computers located in patient care areas will be situated to avoid viewing by patients and visitors. Please refer to [insert title of policy] policy for additional information.
   d. Ensure that secure measures are in place for patients to access their electronic health records (EHRs).7

4. Portable Electronic and Data Devices That Contain Patient Information:
   a. Employees, medical staff members and affiliates are accountable for maintaining the security of patient information that may be contained on laptops, thumb drives and other portable data devices.
   b. Any suspected or actual breaches or threats to the security of portable electronic and data devices must be immediately reported to the appropriate supervisor and to the compliance officer.

5. Patient Education:
   a. Patients will be educated on medical identity theft [state when patients will be educated and how].
   b. Patient education includes, but is not limited to, review of:
      i. A definition of medical identity theft
      ii. How to identify medical identity theft
      iii. How to report actual and/or suspected medical identity theft
iv. The patient’s right to review and correct his/her medical record when discrepancies are identified and how to exercise this right - please refer to the [insert title of policy] policy for additional information.

v. The patient’s right to an accounting of medical record disclosures and how to exercise this right

vi. The importance of guarding insurance card numbers and health insurance records

vii. How to protect their insurance information and personal health information from family and friends

c. Patients will be educated about the Health Insurance Portability and Accountability Act (HIPPA) and standards for privacy.

6. Employee, Medical Staff Member and Affiliate Staff Education:

a. [Insert title of responsible individual] is responsible for developing a training program.

b. Employees, medical staff members and affiliates will be educated on the Program upon hire, on an annual basis and when significant changes have been made to the Program.

c. Education will be provided by [insert title of responsible party].

d. Documentation of the completion of education regarding the Program will be maintained as follows:

i. Employee and affiliate documentation for the completion of education will be maintained in their [insert name of appropriate file].

ii. Medical staff documentation for the completion of education will be maintained in their medical staff office file.

7. Employee, Medical Staff and Affiliate Related Breaches to the Integrity of the Program:

a. Any employee, medical staff member or affiliate who obtains and/or uses patient financial or medical information fraudulently is subject to disciplinary action, including but not limited to, termination and/or revocation of privileges.

b. Fraudulent activities will be reported to law enforcement and other agencies as necessary.

D. Identification, Management and Mitigation of Medical Identity Theft

1. Reporting Suspected and Actual Identity Theft:

a. All employees, medical staff members and affiliates are expected to immediately report verbal or written notice (e.g., patient-generated reports, receipt of a notice of address discrepancy) of suspected or actual identity theft to their immediate supervisor and to the [insert title of responsible individual].

b. The employee, medical staff member or affiliate who receives information regarding suspected or actual identity theft shall complete a Report of Suspected Identity Theft form (See Appendix B) and submit it to the [insert title of responsible individual] the same business day.
2. Patient-generated Reports of Actual or Suspected Medical Identity Theft:
   a. Patient-generated reports of actual or suspected medical identity theft (e.g., receipt of bills for services not rendered, knowledge of someone else using their information to obtain medical services) will be investigated under the direction of the compliance officer.
      i. A written response, including the results of the investigation and actions taken, will be provided to the patient/guardian/surrogate.

3. Investigation of Actual or Suspected Identity Theft:
   a. Investigations will be coordinated by the [insert title of responsible individual].
   b. Upon completion of the investigation, a written report will be completed at the direction of the [insert title of responsible individual] and will include:
      i. Details outlining the investigation
      ii. Measures taken to prevent a recurrence of a similar event, if applicable
      iii. Information regarding reports to law enforcement and/or outside agencies in response to confirmed identity theft
      iv. Information regarding all communications made to the patient/guardian/surrogate

4. External Reporting of Confirmed Identity Theft:
   a. [Insert name of hospital/provider here]'s Program will comply with state data security breach notification laws.
   b. Confirmed medical identity theft shall be reported to law enforcement and appropriate agencies, at the direction of the [insert title of responsible individual].
   c. NOTE: Receipt of a Notice of Address Discrepancy from a credit bureau will trigger an investigation.

5. Police and/or Agency Requests for Information and/or Investigation of Actual or Suspected Identity Theft:
   a. Requests for medical record information and/or billing/financial information (without a court order/subpoena) require the patient’s authorization for release of medical information, according to [insert title of policy] policy.
   b. Any employee receiving a police or agency request for information and/or investigation shall immediately report it to the appropriate supervisor and to the [insert title of responsible individual].
   c. A Report of Suspected Identity Theft form shall be completed following police or agency requests for investigation.

6. Medical Record Corrections:
   a. Please refer to the [insert title of policy] policy, which outlines patient rights under HIPAA, including the patient’s right to request a correction/amendment to his/her medical records and the patient’s right to an accounting of medical record disclosures.
   b. When incorrect information is identified in the patient’s medical record as the result of actual or suspected fraudulent activities, the medical record will be corrected according to HIPAA guidelines and according to the [insert title of policy] policy.
c. The patient will be notified when corrections are made to his/her medical record, according to [insert title of policy] policy.

d. An alert will be placed in the patient’s medical record to caution healthcare providers that a correction/amendment has been made to the patient’s medical record.

E. Service Provider Arrangements/Contractor Compliance
1. [Insert title of responsible individual] is responsible for the oversight of service provider arrangements in compliance with the Federal Trade Commission’s Identity Theft Red Flags Rule.

2. [Insert name of hospital/provider here] will require, by contract, that the contractors, business associates and other service providers that perform activities in connection with “covered accounts” have policies and procedures in place that are designed to detect, prevent and mitigate the risk of identity theft with regard to “covered accounts.”

F. The Role of the Program Committee
1. The Committee shall develop and present the initial Program to the governing body for approval.

2. The Committee shall update the Program on an annual basis and as needed to reflect changes in methods to prevent, identify and mitigate medical identity theft.

3. Committee activities include, but are not limited to:
   a. Coordinating the annual medical identity theft risk assessment
      i. The Committee will evaluate the information gathered, determine potential areas for improvement, coordinate implementation of appropriate measures, and evaluate the effectiveness of the actions taken.
      ii. A summary of the risk assessment will be presented in a written report.
   b. Reviewing reported actual and suspected medical identity theft events
   c. Implementing measures to address events related to medical identity theft, including an evaluation of the effectiveness of actions taken
   d. Conducting and/or facilitating ongoing research to identify changes in methods to prevent, identify and mitigate medical identity theft

4. The Committee shall report to the governing body, at least annually:
   a. Reports summarizing actual and suspected medical identity theft events (including actions taken and an evaluation of the effectiveness of actions taken)
   b. Reports summarizing Committee activities, including activities to mitigate the risk of medical identity theft
   c. Reports summarizing the annual risk assessment (including actions taken and an evaluation of the effectiveness of actions taken)
   d. Proposed updates to the Program

G. The Role of the Governing Body
1. The governing body shall review and approve the initial Program.

2. The governing body will review and approve all revisions to the Program.
Medical Identity Theft Prevention Policy – SAMPLE

3. The governing body shall review Committee activities and a summary of medical identity theft reports on an annual basis and as determined by the Committee.

[Insert name of hospital/provider here] takes medical identity theft very seriously and is committed to ensuring appropriate security measures are in place to prevent medical identity theft and fraudulent use of information.

____________________________________
Chief Executive Officer Signature   Date

____________________________________
[Title of responsible party] Signature   Date

This Program has been approved by the governing body on [insert date].

References:
2. 16 CFR § 681.1(b)(3).
5. Ibid.
6. 16 CFR § 681.1(b)(3).
9. Ibid. p. 17.