THE CHILDREN'S MERCY HOSPITAL
ADMINISTRATIVE POLICY

TITLE: Identity Theft Prevention Program
EFFECTIVE: 11/2008
REVISION DATE:
REVIEWED WITH NO CHANGES: 12/2013
RETIRED:

PURPOSE: The Identity Theft Prevention Program (Program), is designed to detect, prevent and mitigate identity theft in connection with any patient's or other person's Covered Accounts (as defined below).

SCOPE: Children's Mercy Hospital, Children's Mercy South Hospital, Children's Mercy Clinics

ACCOUNTABILITIES/RESPONSIBILITIES: Corporate Compliance

POLICY STATEMENT:

Providing identification is not a condition for obtaining emergency care. The process of confirming a patient's identity must never delay the provision of an appropriate medical screening examination or necessary stabilizing treatment for emergency medical conditions.

I. Identifying and Detecting Red Flags

A. CMH strives to prevent the intentional or inadvertent misuse of patient names, identities, and medical records; report criminal activity relating to identity theft and theft of services to appropriate authorities; and take steps to correct and/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

B. It is the responsibility of any employee who deals with Covered Accounts to take reasonable action to identify Red Flags. When establishing a Covered Account, the employee must properly identify the person for whom the account is opened by comparing the information provided with the information on file. Any suspicious discrepancies should be immediately reported to the employee's supervisor, manager, or director.

C. Examples of potential Red Flags include but are not limited to:

1. An internal report of a lost, stolen or misdirected birth certificate, social security number, current pay stub, tax documents and bank statements of patients or patient family members applying for financial assistance.

2. An internal report that a patient, patient representative, or guarantor's credit card information has been left unattended, lost, misplaced, or stolen.

3. Contact by an individual, other than the patient or guarantor, requesting to obtain personal information on Covered Accounts, including but not limited to prior forms of payment, social security number, address, date of birth, or credit card information.

4. Contact by an individual reporting to be the attorney of the patient, guarantor, or patient representative requesting detailed patient information without proper release of authorization or subpoena on record.

5. A report from a patient, patient representative, or guarantor that he or she has been the victim of identity theft or possible identity theft through lost or misplaced items containing identity information.

6. Presentation of suspicious or altered documents.

7. Notice from law enforcement authorities or other persons regarding possible identity theft in connection with patient accounts.

8. Notice from the parent, patient representative, or guarantor that he or she is not receiving statements on a Covered Account.

9. See Appendix A – Attachment A – Relevant Identity Theft Red Flags Mitigation and Resolution Procedures.

II. Reporting

A. All employees are responsible for notifying their direct supervisor, manager, or director of any circumstances that arise with respect to a Covered Account that creates doubt or suspicion regarding the integrity and accuracy of the information provided. Department management is responsible for communicating staff-identified red flags to the Compliance Office.

III. Preventing and Mitigating Identity Theft

A. In concert with the Compliance Office, the supervisor, manager, or director will take reasonable steps as may be necessary to prevent or mitigate identity theft, including but not limited to the following:

1. Changing any compromised sources of access to the Covered Account.

2. Foregoing attempts to collect on the compromised Covered Account until identity theft concerns are resolved.

3. Notifying the appropriate law enforcement agencies.

4. Informing the victim of the discovery of the identity theft and working with the victim to correct any resulting adverse consequences.

5. Determining that no action is necessary.

6. See Appendix A – Attachment A – Relevant Identity Theft Red Flags Mitigation and Resolution Procedures.

IV. Program Administration and Update

A. This Program is administered by the Corporate Compliance Office.

B. This Program is intended to evolve over time in order to meet changing circumstances, including CMH's experience with identity theft, changes in the nature of and methods used in identity theft and the means for detecting, preventing, and mitigating it, and changes in the nature of Covered Accounts offered by CMH.

DEFINITIONS:

Covered Account: Any account, record, or arrangement that allows a person to make multiple payments to CMH or that involves a foreseeable risk to the safety of CMH patients, staff, or other constituents as a result of identity theft. The most common Covered Accounts include patient accounts placed on deferred payment plans for healthcare services provided by CMH.

Identity Theft: Fraud that involves the use of another's identification (including name, social security number, date of birth, and/or beneficiary or insurance information) to obtain something of value, including medical services.

Red Flag: A pattern, practice, or activity that indicates the possible existence of identity theft.

EXCEPTIONS: requests for exceptions should be directed to the VP, Audit and Compliance.

RELATED POLICIES:

Emergency Medical Treatment and Active Labor Act (EMTALA)

Amending Protected Health Information

Resolution of Compliance Concerns

RELATED FORMS:

See Appendix A – Attachment A – Relevant Identity Theft Red Flags Mitigation and Resolution Procedures.

REFERENCES:

REGULATIONS:

Fair and Accurate Credit Transaction Act of 2003 – Section 114

POLICY CONTENT OWNER: Kristie Michiels, Director of Patient Financial Services

ADMINISTRATIVE COUNCIL SPONSOR: Laurisa Jackson, VP, Finance

REVIEWED BY:
Patricia Madson, Senior Manager, Patient Financial Services

REVIEW PERIOD: 3 years unless required more frequently by regulatory or accreditation requirements.

APPROVED:

Medical Staff Executive Committee:	6/3/2009
Administrative Council:	6/4/2009
Board of Directors:	6/16/2009

NOTE: Formatting changes only for 2013 review**.**

N/A
Medical Staff President — Date

12/12/2013
Randall L. O'Donnell, Ph.D. — Date
President/Chief Executive Officer

Attachment A

Relevant Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flag	Prevention / Mitigation Procedure	Resolution of Red Flag
Documents provided for identification appear to have been altered or forged.	Admissions ("ADM") process will continue but appropriate member of management team will be notified to investigate. ADM will obtain a copy of the individual presenting the documents driver's license and copies of the suspect documents. ADM Management will notify Patient Financial Services ("PFS") Management if billing process should be placed on hold during investigation. ADM will notify Compliance of the incident.	Additional documentation must be provided to resolve discrepancy and continue admissions / billing process.
Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the patient. For example, there is a lack of correlation between the Social Security Number (SSN) range and date of birth.	Admissions process will continue but appropriate member of management team will be notified to investigate. ADM will obtain a copy of the individual presenting the documents driver's license and copies of the suspect documents. ADM Management will notify PFS Management if billing process should be placed on hold during investigation. ADM will notify Compliance of the incident.	Additional documentation must be provided to resolve discrepancy and continue admissions / billing process.
The SSN provided is the same as that submitted by other persons opening an account or other customers.	Admissions process will continue but appropriate member of management team will be notified to investigate. ADM will obtain a copy of the individual presenting the documents driver's license and copies of the suspect documents. ADM Management will notify PFS Management if billing process should be placed on hold during investigation. If after further investigation this is not an error, ADM will notify Compliance of the incident.	Additional documentation must be provided to resolve discrepancy and continue admissions / billing process.
Patient has an insurance number but never produces an insurance card or other physical documentation of insurance.	Admissions process will continue but appropriate member of management team will be notified to investigate. ADM Management will notify Compliance of the incident and will notify PFS Management if billing process should be placed on hold during investigation.	Additional documentation must be provided to resolve discrepancy and continue admissions / billing process. Contact insurance company as necessary. If the results of the investigation

		do not indicate fraud, all contact and identifying information is re-verified with patient.
Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient (e.g., inconsistent blood type).	Clinical staff will notify medical records staff to investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: blood type, age, race, and other physical descriptions may be evidence of medical identity theft. Medical Records staff will obtain a photo of the patient for the record and copies of the parent/guardian identification. If identity theft has occurred, Medical Records will review the complete record for accuracy and modify the record to ensure correct medical information is contained in the patient record. ADM Management will notify PFS Management if billing process should be placed on hold during investigation. ADM will notify the Compliance department.	Depending on the inconsistency and review of the previous file, either delay / do not open a new covered account, or terminate services. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint / inquiry from an individual based on 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 a notice of insurance benefits (or Explanation of Benefits) for health services never received.	PFS staff will notify PFS Management to investigate complaint, interview individuals as appropriate. PFS Management will then notify the Compliance department.	Terminate credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement and financial institutions as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint / inquiry from a patient about information added to a credit report by a health care provider or insurer.	PFS staff will notify PFS Management to investigate complaint, interview individuals as appropriate. PFS Management will then notify the Compliance Department.	Terminate treatment / credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement and financial institutions as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.

Complaint or question from a patient about the receipt of a collection notice from a bill collector.	PFS staff will notify PFS Management to investigate complaint, interview individuals as appropriate. PFS Management will then notify the Compliance Department.	Terminate treatment / credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement and financial institutions as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.	ADM or PFS staff will notify their appropriate Management to investigate complaint. If ADM or PFS Management determines that identity theft or fraudulent activities have occurred, the Compliance Department will be notified.	Additional documentation must be provided to resolve discrepancy and continue admissions / billing process. Contact insurance company as necessary. Notify law enforcement and financial institutions as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.	Bad Address/Returned Mail procedures are used to find the patient's current mailing address. If fraudulent activity is suspected, the Compliance Department will be notified by PFS.	Patient is found and contact information is updated.
Hospital is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.	ADM or PFS staff will investigate to determine if billing was made fraudulently. ADM or PFS Management will then the Compliance Department.	Additional documentation must be provided to resolve discrepancy and continue admissions / billing process. Contact insurance company as necessary. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Personal identifying information provided by the patient is associated with known fraudulent activity as indicated by internal or third	ADM or PFS staff will notify their appropriate Management to investigate complaint. ADM will obtain a copy of the	Terminate treatment / credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been

– party sources used by the Hospital. For example: - The address on an application is the same address provided on a fraudulent application; or The phone number on an application is the same as the number provided on a fraudulent application.	individual presenting the documents driver's license and copies of the suspect documents. ADM or PFS Management will then notify CMH Compliance Officer.	resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.