St. Joseph's Health

RED FLAGS IDENTITY THEFT PREVENTION

Policies and Procedures

Department: CORPORATE COMPLIANCE

PURPOSE:

The St. Joseph's Healthcare System's Red Flag Identity Theft Prevention Program is designed to reduce the risk of identity theft through detection, prevention and mitigation of patterns, practices or activities ("Red Flags") that could be indicative of potential identity theft.

APPLICABILITY:

- St. Joseph's Health System
- St. Joseph's University Medical Center
- St. Joseph's Children's Hospital
- St. Joseph's Healthcare and Rehab Center
- St. Joseph's Wayne Medical Center

DEFINITIONS:

Identity theft: fraud that involves stealing money or getting other benefits by using the identifying information of another person.

POLICY:

It is the policy of St. Joseph's Healthcare System ("SJH") to follow all federal and state laws and reporting requirements regarding identity theft. SJH shall identify and respond to Red Flags which may indicate potential identity theft.

Identification of Red Flags

In the course of caring for patients, SJH employees and physicians may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. SJH identifies the following as potential red flags:

1. A complaint or question from a patient based on the patient's receipt of:

a. A bill for another individual;

b. A bill for a product or service that the patient denies receiving;

c. A bill from a health care provider that the patient never patronized; or

d. A notice of insurance benefits (or explanation of benefits) for health care services never received.

2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.

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

4. A patient or health insurer report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.

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

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

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

8. A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud agency.

Detecting Red Flags

SJH staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. Staff will verify patient identity, address and insurance coverage at the time of patient registration.

1. SJH Emergency Departments* and all other registration/intake areas must review and include in each patient's file a photo ID issued by a local, state, or federal government agency (e.g., a driver's license; passport; military ID, etc.).

a. In the event the patient does not have photo ID, ask for two forms of non-photo ID, one of which has been issued by a state or federal agency (e.g., Social Security card and a utility bill or company or school identification).

b. When the patient is under 18 or if the patient is unable due to their condition to produce identification, the responsible party's identification shall be requested.

2. Each time a patient visits, check whether the identification provided is valid, copy the identification provided, and match any photo to the patient/responsible party.

3. Responding to Questions. If asked the reason for the identifying procedures, explain that the procedures are "for patient protection to prevent identity theft and theft of services." Politely remind questioners this is the same process used to cash a check, make a large credit card purchase, or board a plane.

4. Refusal to Provide or Lack of Identification. No one should be refused care because they do not have acceptable identification with them. Patients should be asked to bring appropriate documents to their next visit.

***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.**

Responding to Red Flags

If an employee detects fraudulent activity or if a patient claims to be a victim of identity theft, SJH will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, SJH will also apply its existing HIPAA security policies and procedures to the response.

If potentially fraudulent activity (a red flag) is detected by a SJH staff member:

1. The staff member shall gather all documentation and report the incident to his or her immediate supervisor.

2. The supervisor shall assess the situation to determine if potential identity theft exists.

a. The assessment may determine that no risk of identity theft is present (i.e. a mistake has occurred, or the occurrence is readily explainable).

b. If, after preliminary investigation, the supervisor suspects identity theft may have occurred, he/she shall notify a Manager in Patient Financial Services who shall place a collection hold on the account and enter a Red Flag in Soarian Financials. Security Dispatch, Corporate Compliance and/or Legal Affairs must also be notified of all suspected incidents of identity theft.

If a patient claims to be a victim of identity theft:

1. SJH staff must report all patient claims of identity theft to Corporate Compliance.
2. The patient should be encouraged to file a police report for identity theft if he/she has not done so already.
3. Corporate Compliance staff shall send written acknowledgement (see EXHIBIT A) to the patient with a copy of the Federal Trade Commission (FTC) Identity Theft affidavit (EXHIBIT B) enclosed.
    a. Unless there is actual knowledge that identity theft has occurred at an SJH facility, SJH must receive a properly completed and signed FTC Identity Theft Affidavit before correcting medical or payment records or proceeding with other victim assistance steps under this policy.
    b. Once an FTC Identify Theft Affidavit supports the identity theft allegation, the facility must flag the account of the patient alleging identity theft so that registration and medical personnel are alert to the issue that the medical record may contain inaccurate information about the patient. SJH will compare the patient's documentation with personal information in the Hospital's records.
4. The Patient Financial Services Director will put all patient accounts potentially affected by the alleged identity theft on hold pending the outcome of the investigation.

If, following investigation, it appears that a patient has been a victim of identity theft:

Corporate Compliance staff will promptly consider what further remedial act/notifications may be needed under the circumstances.

a. The physician will review the affected patient's medical record to confirm whether documentation was made in the patient's medical record that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.
b. The HIM/Medical Records staff will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action taken.
c. The billing department will make appropriate corrections to the patient's billing information, inform and provide documentation to any third-party payer affected by the adjustments, and make any necessary repayments to ensure that the patient and the payer pay only for services actually provided to the patient.
d. Accounting for Disclosures. Corporate Compliance staff should determine whether, as result of patient misidentification, protected health information was inappropriately disclosed. If PHI was inappropriately disclosed, the HIM department must account for such disclosure in accordance with federal and state law and SJH policy.
e. External notification and reporting will occur only as directed by the General Counsel.
    i. Reporting Medicaid Fraud. When there is actual knowledge of Medicaid fraud (e.g., a patient uses another person's Medicaid information to obtain medical care), the fraud must be reported immediately to the Medicaid OIG: 1-866-633-6585.

If following investigation, it does not appear that the patient has been a victim of identity theft: SJH will take whatever action it deems appropriate including, but not limited to, removal of Red Flag in Soarian Financials.