IDENTITY THEFT RED FLAGS RULE POLICY

Scope:
LSUHSC-Shreveport which includes facilities and providers at all Shreveport, EA Conway, and Huey P Long Campuses.

Purpose:
As an issuer of credit to recipients of its healthcare services, LSUHSC-Shreveport adopts an Identity Theft Prevention Program (Program) to assist in identifying, detecting, and mitigating risks of identity theft affecting patients of the Hospital. This policy is intended to comply with requirements of Federal Trade Commission's Identity Theft Prevention Red Flag Rules - 16 C.F.R. Section 681.2 (2008) which is a result of the Fair and Accurate Credit Transactions (FACT) Act of 2003.

Policy:
It is LSUHSC-S intent to provide safeguards to protect patients by detecting Red Flags and preventing or mitigating Identity Theft without impacting appropriate care of patients or compliance with the Emergency Medical Treatment and Active Labor Act (EMTALA).

Definitions:

I. Identity theft - fraudulently using the identifying information of another person.

II. Medical Identity Theft - When an individual assumes or attempts to assume the identity of another person through fraudulent means or false pretenses and obtains or attempts to obtain medical service or goods, or to make false claims for medical services or goods.

III. Red Flag - a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Procedure:

I. IDENTIFICATION OF RED FLAGS

Activities involving Identity Theft generally fall within one of the following general types of red flags:
A. Suspicious documents
B. Suspicious personal identifying information, such as a suspicious address
C. Unusual use of – or suspicious activity relating to – a covered account
D. Alerts from others (e.g. customer, identity theft victim, or law enforcement)

II. DETECTECTION OF RED FLAGS
A. LSUHSC-S has adopted the following procedures to aid in the detection of red flags for identity theft:

1. New Patient Accounts
   Obtain appropriate identifying information and insurance information. This should include the following:
   a. Full legal name
   b. Date of Birth
   c. Address
   d. Government issued or other valid picture ID
   e. When applicable, patient’s insurance card, etc. (when possible, verify the insurance company’s information)

2. Existing Patient Account
   a. During each return patient registration have patient show a picture ID, and update the personal and insurance information listed above.
   b. Verify validity of requests for changes of billing addresses.
   c. Verify identification of patients before releasing any personal information.

3. Emergency Care – No Delay
   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.

III. PREVENTION AND MITIGATION OF IDENTITY THEFT

A. If a patient notifies LSUHSC-S of possible identity theft in regard to their medical record or bill, an investigation will be coordinated with the appropriate department(s) (e.g., Patient Financial Services and Medical Records) pursuant to LSUHSC-S established departmental procedures.

B. In determining an appropriate response to a red flag or other threat of identity theft, LSUHSC-S will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a patient’s account records, or notice that a patient has become aware of someone fraudulently claiming to obtain medical services in the name of the patient.

C. Appropriate responses may include:
   1. Monitoring a covered account for evidence of identity theft;
   2. Contacting the patient;
   3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
   4. Reopening a covered account with a new account number;
   5. Not opening a new covered account;
   6. Closing an existing covered account;
   7. Notifying law enforcement; or
   8. Determining that no response is warranted under the particular circumstances.
D. Internal Notifications:
   Any LSUHSC-S employee who becomes aware of a potential or actual breach of personal information should report it to their manager for follow-up. The Compliance Office should be notified of all breaches and resolutions.

E. External Notification:
   The Compliance Office will work with the appropriate department(s) to determine if any reports to outside agencies are required.

IV. UPDATING THE PROGRAM
   LSUHSC-S will evaluate and update policies and procedures as necessary to reflect changes in risks to patients or to the organization from identity theft.

V. PROGRAM OVERSIGHT
   The Compliance Office shall report to the Board, at least annually, on LSUHSC-S’s compliance with the identity theft program.

_______________________
Administrator

10/18/12
Date

Approved by Clinical Board: 8/18/09, 10/16/12
Written: 7/09
Revised:
Reviewed: 10/12