Stony Brook Medicine Administrative Policy and Procedures

Subject: LD0080 Identity Theft Prevention, Detection and Mitigation: Red Flag Alert	**Published Date:** 04/17/2015
Leadership	**Next Review Date:** 04/17/2018
Scope: Hospital Wide	**Original Creation Date:** 11/04/2011

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Responsible Department/Division/Committee:

Compliance

Policy:

Stony Brook University Hospital (SBUH), in compliance with the Federal Trade Commission (FTC) Red Flag Rule, will utilize the procedures that follow to prevent, detect and mitigate potential or actual identity theft/fraudulent use of an individual's identity.

Definitions:

Identity Theft: The use of another individual's identifying information, for personal gain or benefit, by pretending to be that individual.

Covered Account: An individual patient account that allows periodic crediting activity for services rendered including, but not limited to, deferred payments or poses a reasonably foreseeable risk of being used to promote identity theft

Responsible Staff: SBUH workforce members based on title/role function, who undertake activities relating to Patient Accounts and are responsible for performing the day-to-day procedures defined in this policy to prevent, detect and respond to red flag alerts.

Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft or fraudulent use of an individual's identity.

Photo ID: Government issued photo ID such as a state issued drivers license or in the event the pt. does not have a government photo ID, two other forms of ID, one of which must be a government issued ID, such as a social security card in addition to a utility bill or company/school ID which may contain a photo to assist with proper identification of the patient.

Procedures:

A. Identification of a Red Flag

SBUH responsible staff will identify potential or actual red flags in one of the following manners:

1. Presentation of suspicious documents by an individual presenting for health care services (photo ID information not consistent with existing documentation).

2. The use of suspicious personal identifying information or inability to confirm identifying information (Individual unable to provide/confirm current or previous identifying information such as address, phone number, date of birth, social security number, insurance information, etc.).

3. Suspicious or unusual use of a Patient account.

4. Receipt of alerts from other sources such as an individual patient reporting identity theft, law enforcement, consumer reporting agencies or services providers (credit freeze, fraud alert or address discrepancy).

B. Detection of a Red Flag

In order to facilitate the detection of the Red Flags identified in the table attached, responsible staff will take the following steps to obtain and verify the identity of the individual patient presenting for health care services:

1. All new patients at the time of registration will be required to submit at a minimum the following identifying information: full name, date of birth, address, phone, etc., along with a current government issued photo ID * and insurance card, if applicable, which will be scanned via RASi to the file

2. All existing patients at the time of registration are required to provide their full name, date of birth, address, phone, etc., along with a current government issued photo ID * and insurance card, if applicable, which will be validated against existing documentation in Siemens and RASi,

only when identifying information is unable to be verified by the individual or when a Red Flag Alert exist on the record.

3. For patients who refuse or are unable to provide adequate photo ID* continue registration and place alert in the red-flag field. If the patient continues to refuse or not provide adequate photo ID* upon subsequent visits, notify the Compliance Officer.

4. All existing patients requesting changes to identifying information (such as name and/or address changes) are required to provide documents to authenticate the validity of the request.

5. In the event the pt. does not have a government photo ID, ask for two other forms of ID, one of which must be a government issued ID, such as a social security card in addition to a utility bill or company/school ID which may contain a photo to assist with proper identification of the patient.

C. Preventing and Mitigating Identity Theft

In order to prevent and mitigate the effects of identity theft, responsible staff will follow the appropriate steps identified in the table (refer to the attachment below) and update/correct, as necessary, patient registration information in Siemens.

D. Service Provider Arrangements

All Business Associates that perform activities in connection with Patient Accounts will be required by contract, to have policies and procedures in place designed to detect, prevent and mitigate the risk of identity theft with regard to the Patient Accounts.

E. Questions

Any questions about this policy should be directed to the Director of Patient Access Services or the Director of Patient Accounting Services or the Compliance Officer.

Forms: (Ctrl-Click form name to view)

Identity Theft Red Flags Mitigation and Resolution Procedures

Policy Cross Reference: (Ctrl-Click policy name to view)

None

Relevant Standards/Codes/Rules/Regulations/Statutes:

Fair and Accurate Credit Transaction Act 2003 §114, 315 and Federal Trade Commission’s Identity Theft Prevention red Flags Rule 16 CFR § 681.2

References and Resources:

None