Stony Brook Medicine Administrative Policy and Procedures

Subject: LD0080 Identity Theft Prevention, Detection and Mitigation: Red Flag Alert	**Published Date:** 12/07/2022
Leadership	**Next Review Date:** 12/07/2025
Scope: SBM Stony Brook Campus	**Original Creation Date:** 11/04/2011

Responsible Department/Division/Committee:
Office of Compliance and Audit Services (OCAS)

Policy:
Stony Brook University Hospital (SBUH) is committed to preventing, detecting and mitigating the intentional or inadvertent misuse of patient names, identities, identifying information and medical records; reporting criminal activity related to identity theft and theft of services to appropriate authorities; and taking steps to correct and/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately. SBUH requires staff and employees to appropriately identify patients and confirm personal demographic information as well as insurance information at the time of registration for each patient visit, during treatment, at time of billing, and before confidential patient information can be released.

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

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 identified "Possible Red Flags."

Possible Red Flags: 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 identification document such as a state issued driver's license, government issued passport, or in the event the patient does not have a government photo ID, two other forms of identification, one of which must

be government issued, 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.

Patient: "Patient" refers to the patient, parent or guardian of a minor patient, guardian or personal representative of an incapacitated adult patient.

Procedures:

A. Identity Theft Possible Red Flags Mitigation and Resolution Procedures

Identity Theft Possible Red Flag	Mitigation Procedure/Resolution of Red Flag or Recommended Action Taken
1) Documents provided for identification appear to have been altered or forged. 2) Personal identifying information provided by the patient/parent/ guardian or patient representative is not consistent with other personal identifying information provided by the patient. For example, there is a lack of correlation between Social Security Number (SSN) range and the date of birth. 3) The SSN provided is the same as that submitted by another patient.	Patient Access requires the patient to provide additional satisfactory documented information to verify identity and resolve discrepancy. In the absence of documentation resolving the discrepancy: If an established patient, in emergent situations, continue registration process by assigning a new Medical Record Number (MRN), placing "Possible Identity Fraud" alert in the notification section, and marking 'yes' in the "Possible Red Flag" field. This ensures that (1) the Patient Access QA team conducts a formal investigation and issues a report summary to the OCAS; (2) the OCAS notifies Patient Accounts to place the account on hold pending the outcome of the investigation; (3) OCAS confirms or removes the "Possible Red Flag" and (4) the OCAS takes any further action necessary. **Please Note:** For electives, begin investigation as soon as possible. Ideally before admission or encounter

4) Name on insurance card, name on identification, and name given by patient are discrepant.	Patient Access requires the patient to provide additional satisfactory documented information to verify identity and resolve discrepancy. If unable to verify insurance coverage, register as self-pay and advise patient. If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with the patient. In the absence of documentation resolving the discrepancy for an established patient, in emergent situations, continue registration process by assigning a new MRN, placing "Possible Identity Fraud" alert in the notification section and marking 'yes' in the "Possible Red Flag" field. This ensures that (1) the Patient Access QA team conducts a formal investigation and issues a report summary to the OCAS; (2) the OCAS notifies Patient Accounts to place the account on hold pending the outcome of the investigation; (3) OCAS confirms or removes the "Possible Red Flag" and (4) the OCAS takes any further action necessary. **Please Note:** For electives, begin investigation as soon as possible. Ideally before admission or encounter.

5) Records indicate a medical treatment that is inconsistent with a physical examination or with a medical history as reported previously by the patient (i,e. blood type or x-rays do not match).	The clinician shall continue to treat the patient and monitor the account for evidence of identity theft. For example, verifying the individual's identity, each time the individual presents for health care services, against the scanned photo ID*. **Please Note**: When and only when there is an emergent reason to combine or un-combine MRNs, the clinician may contact Patient Access Bed Control 24 hours/7days a week via phone at extension 42591. When the information is determined to be inconsistent send an email to: PatientAccessQA@stonybrookmedicine.edu with copies to, Director of Patient Access Services, Senior Manager Registration QA, and SBUH_OCAS_Compliance_Staff@stonybrookmedicine.edu requesting to update the encounter for the patient as a "Possible Identity Fraud" alert and "Possible Red Flag." The email should include the following: ○ MRN ○ Financial Number ○ Last Name, First Name ○ Date of Birth ○ Any other pertinent details regarding the inconsistency This ensures that (1) Patient Access flags the encounter; (2) the Patient Access QA team conducts a formal investigation and issues a report summary to the OCAS; (3) the OCAS notifies Patient Accounts to place account on hold pending the outcome of the investigation; (4) OCAS confirms or removes the "Possible Red Flag" and (5) the OCAS takes any further action necessary.

*****In the event the patient 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.

Identity Theft Possible Red Flag	Mitigation Procedure/Resolution of Red Flag or Recommended Action Taken
6) Complaint/inquiry from an individual based on receipt of: • A bill for another individual; • A bill for a product or services that the patient denies receiving; • A bill from a health care provider that the patient denies patronizing; • A notice of insurance benefit or explanation of benefits (EOB) for health services never received or inconsistent with the patient's medical history/condition 7) Complaint/inquiry from a patient about information added to a credit report by a health care provider or insurer where the patient alleges the situation is consistent with those outlined in #6 above. 8) Complaint/inquiry from a patient about information added to a credit report by a health care provider or insurer where the patient alleges the situation is consistent with those outlined in #6 above. 9) Patient or insurance company report that coverage for legitimate hospital stay is denied because insurance benefits have been depleted or lifetime cap has been reached and previous services were never received. 10) Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's account. 11) SBUH is notified by a patient, or a victim of identity theft, or law enforcement, or other appropriate authority that the Hospital has opened a fraudulent account for a person engaging in identity theft.	Any responsible staff who become aware of a possible red flag is required to send an email to PatientAccessQA@stonybrookmedicine.edu with copies to, Director of Patient Access Services, Senior Manager Registration, QA, and SBUH_OCAS_Compliance_Staff@stonybrookmedicine.edu requesting to update the encounter for the patient as a "Possible Identity Fraud" alert and "Possible Red Flag." The email should include the following: ○ MRN ○ Financial Number ○ Last Name, First Name ○ Date of Birth ○ Any other pertinent details regarding the possible identity fraud This ensures that Patient Access (1) flags the encounter; (2) the Patient Access QA team conducts a formal investigation and issues a report summary to the OCAS; (3) the OCAS notifies Patient Accounts to place the account on hold pending the outcome of the investigation; (4) OCAS confirms or denies the "Possible Red Flag" and (5) the OCAS takes any further action necessary.

12) Personal identifying information provided by the patient is associated with known fraudulent activity as indicated by internal or third-party sources used by SBUH. For example, same SSN is provided by several different patients.	

B. Patient Financial Services Workflow

After a "Red Flag" has been confirmed by OCAS, Patient Financial Services will review and send all future encounters related to the identified patient's MR to OCAS to confirm whether the claim is appropriate for billing. Additionally, Patient Financial Services will regularly check the "Red Flag Work List" to ensure there are no issues regarding any previously confirmed "Red Flags."

C. Service Provider Arrangements

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

D. Questions

For questions pertaining to this policy, contact the Director of Patient Access Services or the Chief Compliance Officer.

Forms: (Ctrl-Click form name to view)
None

Policy Cross Reference: (Ctrl-Click policy name to view)
RI0035 Patient Identification

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