Stony Brook Southampton Hospital
A Location of Stony Brook University Hospital

Stony Brook Medicine
Administrative Policy and Procedures

Subject: HLD0080 Identity Theft Prevention, Detection and Mitigation: Red Flag Alert	**Published Date:** 08/21/2025
Leadership	**Next Review Date:** 08/21/2026
Scope: SBM Southampton Campus	**Original Creation Date:** 05/17/2018

Policy:

Stony Brook University Hospital (including all campus locations, collectively 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 workforce members 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:

Authorized Representative: An individual legally empowered to provide permission, consent or action on behalf of a patient often referred to as a health care proxy, health care agent, administrator, appointed representative, personal representative, executor/executrix, surrogate decision maker, court appointed guardian/agent or power of attorney specific to health care.

Authorized Provider - A member of the medical staff, resident/fellow physician, nurse practitioner or physician assistant permitted by law and Stony Brook University Hospital (SBUH) to provide medical care, treatment and services within the scope of licensure and/or consistent with individually granted privileges.

Identity Theft: The use of another individual's identifying information, for

personal gain or benefit, by pretending to be that individual.

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

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. For the purpose patient Identification government issued photo IDs include:

- Passport;
- US Permanent Residency Card, (Green Card);
- Certificate of Naturalization (N550-570) or Certificate of US Citizenship (N 560-561);
- US Work Visa;
- Certificate of Degree of Indian Blood or other US American Indian/Alaska Native Tribal document with photo;
- Driver's License/State identification;
- U.S. Military Card; 8. U.S. Military Dependent's Card.

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."

Stony Brook University Hospital campus locations -

Stony Brook University Hospital Main Campus (SBUH Main Campus)
Stony Brook Eastern Long Island Hospital (SBELIH)
Stony Brook Southampton Hospital (SBSH)

Workforce Member: An employee, volunteer, trainee, medical staff member, including state, research foundation, professional employer organization, personnel employed through contracted agencies, or other

individual affiliated with SBUH who furnish products or services on behalf of SBUH or is otherwise under the direct control of SBUH, regardless of whether they receive(d) payment(s) from SBUH.

Procedures:

I. SBUH employs Preventive, Detective, Mitigation and Resolution Procedures addressing scenario-specific Possible Red Flags

A. **Identity Theft: Possible Red Flags Related to Identification: Scenarios and Corresponding Mitigation Procedure/Resolution**

1. Scenarios:

i. Documents provided for identification appear to have been altered or forged.

ii. Personal identifying information provided by the patient/parent/guardian or authorized 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.

iii. The SSN provided is the same as that submitted by another patient.

2. SBUH workforce member Mitigation Procedure/Resolution of Red Flag or Recommended Actions for Possible Red Flags Related to Identification.

i. Refer to HRI0035 Patient Identification to verify identity and resolve discrepancies.
ii. In the absence of documentation in resolving the discrepancy: If an established patient is an emergent situation, continue the registration process by assigning a new patient medical record number and:
iii. **SBUH Main Campus:** - place a "Possible Identity Fraud" alert in the notification section and mark 'yes' in the "Possible Red Flag" field.
v. **SBSH:** Place a note in CPSI of the "Possible Identity Fraud.
vi. **SBELIH:** Contact, the Director of Health Information Management (HIM).
vi. Please Note: For elective treatment or services, begin investigation as soon as possible. Ideally before admission or encounter.

B. **Identity Theft: Possible Red Flags Related to Insurance or Third Party Payment Scenario and Corresponding Mitigation Procedure/Resolution**

1. Scenario

i. Name on insurance card, name on identification, and name given by patient are discrepant.

2. SBUH workforce member Mitigation Procedure/Resolution of Red Flag or Recommended Actions for Possible Red Flags Related to Insurance or Third-Party Payment

i. Refer to HRI0035 Patient Identification for diligent validation process guidelines to Patient Access requires the patient to provide additional satisfactory documented information to verify identity and resolve discrepancies.
ii. If unable to verify insurance coverage, advise patient and register as self-pay. If the results of the investigation do not indicate fraud, re-verify all contact and identifying information with the patient.
iii. **For SBUH campus only -** In the absence of documentation resolving the discrepancy: If 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.
iv. **For SBSH campus only:** In the absence of documentation resolving the discrepancy: If an established patient in an emergent situation, continue registration process by assigning a new Medical Record Number (MRN), and placing a note in CPSI of the "Possible Identity Fraud."
v. **For SBELIH campus only -** In the absence of documentation resolving the discrepancy: If an established patient, in emergent situations, continue the registration process by assigning a new MRN and contact the VP of Quality or Director of Health Information Management.
vi. **Please Note:** For elective treatment or services, begin investigation as soon as possible. Ideally before admission or encounter.

C. **Identity Theft: Possible Red Flags Related to Medical Treatment Records Scenario and Corresponding Mitigation Procedure/Resolution**

1. **Scenario**

i. Patient medical records indicate treatment that is inconsistent with a physical examination or a medical history as reported previously by the patient (i.e. blood type or x-rays do not match).

2. **SBUH workforce member Mitigation Procedure/Resolution of Red Flag or Recommended Actions Related to Medical Treatment Records**

i. The authorized provider continues 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 compared to the scanned photo ID.

a. In the event the patient does not have a government photo ID, ask for two (2) other forms of ID, one (1) 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.

ii. **SBUH Main Campus and SBSH Only**: When and only when there is an emergent reason to combine or un-combine MRNs, the authorized provider contacts:

a. **SBUH Main Campus**: Patient Access Bed Control 24 hours/7days a week via phone at extension 42591.

b. **SBSH:** Patient Access Data Integrity Coordinator, Monday through Friday 8:00am- 4:00pm via email SBSH_PatientAccessQA@stonybrookmedicine.edu or contacting Patient Access QA Manager outside of these hours.

iii. When the information is determined to be inconsistent:

a. **SBUH Main Campus:** send an email: PatientAccessQA@stonybrookmedicine.edu with copies to, Director of Patient Access Services, Senior Manager Registration QA, and SBUH_OCAPS_Compliance_Staff@stonybrookmedicine.edu requesting to update the encounter for the patient as a "Possible Identity Fraud" alert and "Possible Red Flag."

b. **SBSH:** send an email to SBSH_PatientAccessQA@stonybrookmedicine.edu with copies to SBUH OCAPS Compliance Staff@stonybrookmedicine.edu

c. **SBELIH:** contact the Quality Department, Director of Revenue Cycle and send an email to SBUH SBUH_OCAPS_Compliance_Staff@stonybrookmedicine.edu.

iv. The email includes the following presented patient information:
   a. MRN
   b. Account Number/Financial Number
   c. Last Name, First Name
   d. Date of Birth
   e. Any other pertinent details regarding the inconsistency

D. **Identity Theft: Possible Reds Related to Payment, Credit and Financial Services Flag Scenarios and Corresponding Mitigation Procedure**

1. Scenarios

i. Complaint/inquiry from an individual based on receipt of:
   a. A bill for another individual;
   b. A bill for a product or services that the patient denies receiving;
   c. A bill from an authorized provider that the patient denies patronizing; or
   d. A notice of insurance benefit or explanation of benefits (EOB) for health services never received or inconsistent with the patient's medical history/condition.

iii. Complaint/inquiry from a patient about information added to a credit report by an authorized provider or insurer where the patient alleges the situation is consistent with those outlined in D(1)(i) above.

iv. Patient or insurance company report that coverage for legitimate SBUH stay is denied because insurance benefits have been depleted or lifetime cap has been reached and previous services were never received.

v. Mail sent to the patient is returned repeatedly as undeliverable although activity continues in connection with the patient's account.

vi. SBUH is notified by a patient, a victim of identity theft, law enforcement, or other appropriate authority that SBUH has opened a fraudulent account for a person engaging in identity theft.

vii. 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.

2. SBUH workforce member Mitigation Procedure/Resolution of Red Flag or Recommended Actions Related to Payment, Credit and Financial Services Flag Scenarios made the same revisions as previously indicated.

i. Any responsible workforce member that becomes aware of a possible red flag is required to contact/send an email to:
   a. **SBUH Main Campus**: PatientAccessQA@stonybrookmedicine.edu with copies to, Director of Patient Access Services, Senior Manager Registration, QA, and SBUH_OCAPS_Compliance_Staff@stonybrookmedicine.edu requesting to update the encounter for the patient as a "Possible Identity Fraud" alert and "Possible Red Flag."
   b. **SBSH:** SBSH_PatientAccessQA@stonybrookmedicine.edu with copies to SBUH_OCAPS_Compliance_Staff@stonybrookmedicine.edu the director of Patient Access, and the Patient Access QA Manager requesting to update the encounter for the patient in the medical record**.**
   c. **SBELIH:** contact the Director of Revenue Cycle and send an email to SBUH OCAPS SBUH_OCAPS_Compliance_Staff@stonybrookmedicine.edu

ii. The email includes the following presented patient information:
   a. MRN
   b. Account Number/Financial Number
   c. Last Name, First Name
   d. Date of Birth
   e. Any other pertinent details regarding the inconsistency

iii. In the event the patient does not have a government photo ID, ask for two (2) other forms of ID, one (1) 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.

iv. **Identify Theft: Review Process guided by above scenarios**

i. Patient Access flags the encounter;

ii. Patient Access QA/ Quality Services conducts a formal investigation and issues a report summary to the OCAPS;

iii. the OCAPS notifies Patient Accounts/Patient Financial Services to place account on hold pending the outcome of the investigation;

iv. Notification is sent to Risk Management (all) and Privacy Management **(SBSH)** of the "Possible Red Flag" and coordinates further actions as necessary;
v. OCAPS confirms or removes the "Possible Red Flag" and takes any further action necessary.

II. II. Patient Financial Services Workflow

At SBUH after a "Red Flag" has been confirmed by OCAPS, Patient Financial Services reviews and sends all future encounters related to the identified patient's MRN to the OCAPS to confirm whether the claim is appropriate for billing. Additionally, Patient Financial Services regularly checks the "Red Flag Work List" to ensure there are no issues regarding any previously confirmed "Red Flags."

E. Work List Procedure: **SBSH Only:**

On a monthly basis, Patient Access QA updates all "Possible Red flag" encounters on a "Red Flag Work List" granting access to the OCAPS. This ensures OCAPS has current knowledge of all "Possible Red Flags."

F. Service Provider Arrangements

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

I. Questions
a. For questions pertaining to this policy,

SBUH Main Campus and SBSH: contact the Director of Patient Access Services or the Chief Compliance Officer.

SBELIH: contact the Director of Revenue Cycle Services or the Chief Compliance Officer.

Forms: (Ctrl-Click form name to view)

None

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

HRI0035 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