



This document is intended to be a template which should be customized to fit the unique needs of the provider's operations.

## Policy Template – Red Flag Identity Theft Prevention and Detection Procedures

### Policy

Admission and Accounts Receivable staff, or other staff as deemed appropriate, will take reasonable steps to identify, verify and mitigate possible identity theft that may occur during the admission process and on-going accounts receivable transactions with residents and clients who establish and/or maintain an account with the (insert organization name). Red Flags may be detected in obtaining identifying information about, and verifying the identity of, a person opening an account and /or monitoring transactions and verifying the validity of change of address requests, in the case of existing accounts.

#### 1. Identification of Red Flags

**a. The following may be identified during the admission process as a “Red Flag” that may indicate an attempted identity theft.**

- i. A resident who has an insurance number but never produces an insurance card or other physical documentation of insurance.
- ii. Information provided upon admission does not match other sources (i.e., common working file, banking or insurance information, etc.)
- iii. The Medicare # that ends in "a" does not match the social security number provided by the resident. A Medicare # ending in "A" should match the resident's own social security number.
- iv. The presentation of suspicious personal identifying information, such as a suspicious address change or a non-verifiable address such as a PO box.
- v. The presentation of suspicious documents.

If after verifying the information provided or received did not contain an administrative error, the Red Flag must be reported immediately to *[Insert proper individual/department]* for investigation purposes.

**b. The following may be identified during account maintenance as a “Red Flag” that may indicate potential identity theft.**

- i. A complaint or question from a resident based on the resident's receipt of:
  1. a bill for another individual
  2. a bill for a product or service that the resident denies receiving
  3. a bill from a health care provider that the resident never:
    - a. patronized or
    - b. a notice of insurance benefits (or Explanation of Benefits) for health services never received.
- ii. Claim denied due to overlapping dates of service.
  1. The resident may be a victim of identity theft due to another provider billing for services during the same time period.
  2. The resident may be the perpetrator of identity theft and your claim is denied because the true individual has received services from another provider during the same time period.
- iii. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the resident.
- iv. A complaint or question from a resident about the receipt of a collection notice from a bill collector.



**This document is intended to be a template which should be customized to fit the unique needs of the provider's operations.**

- v. A resident or insurance company reports that coverage for legitimate inpatient stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
- vi. A complaint or question from a resident about information added to a credit report by a health care provider or insurer.
- vii. A dispute of a bill by a resident who claims to be the victim of any type of identity theft.
- viii. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.
- ix. Notice from residents, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with accounts.

If after verifying the information provided or received did not contain an administrative error, the Red Flag must be reported immediately to *[Insert proper individual/department]* for investigation purposes.

### **3. Verifying Red Flags to Detect Identity Theft**

- a. Appropriate methods for verifying Red Flags to determine if identity theft has occurred or is occurring may include the following:
  - i. Contacting the resident;
  - ii. Monitoring an account for evidence of identity theft;
  - iii. Contacting the Social Security Office to verify resident identity;
  - iv. Contacting the resident's insurance company to verify payment information; or
  - v. Reviewing the Common Working File for discrepancies in resident data.

### **4. Mitigation/ Response to Red Flags**

- a. Appropriate responses to verified Red Flags should be commensurate with the degree of risk posed. In determining an appropriate response, consideration is given to aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a resident's account records, or notice that a resident has provided information related to an account to someone fraudulently claiming to represent the Company or to a fraudulent website. Appropriate responses may include and are not limited to the following:
  - i. Contacting the resident;
  - ii. Notifying the resident's insurance company;
  - iii. Changing any passwords, security codes, or other security devices that permit access to an account;
  - iv. Notifying law enforcement;
  - v. Determining that no response is warranted under the particular circumstances;
  - vi. Adjusting charges to the covered account that were fraudulently incurred; or
  - vii. Modify identifying information in the record in accordance with Health Information Management policies to prevent the proliferation of fraudulent health information.