

| <b>Comprehensive Behavioral Health Management/College Health IPA<br/>Policy and Procedure Manual</b> |  |
|--|--|
| <b>Policy Name:</b> Identity Theft Prevention  | <b>Security of Personal Health Information</b> |
| <b>Date:</b> 07-09   | <b>Page:</b> 1 of 3                            |
| <b>Reviewed by QI Committee:</b> 07-09, 11-09  | <b>Policy Number:</b> SC-11                    |
| <b>Revised by QI Committee:</b> 11-09  |  |

**Purpose:** To ensure Comprehensive Behavioral Health Management/College Health IPA (CBHM/CHIPA) follows all state and federal laws and reporting requirements regarding identity theft. Specifically, this policy outlines how CBHM/CHIPA will (1) identify, (2) detect and (3) respond to “red flags.” A “red flag” as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft. Pursuant to the existing HIPAA Security Rule, appropriate physical, administrative and technical safeguards will be in place to reasonably safeguard protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure.

**Policy:**

1.0 Oversight

The CBHM/CHIPA Vice-President of Financial Operations is responsible for oversight of the security program. The Vice-President of Financial Operations works closely with the Vice-President of Clinical Services and the Vice-President of Product Management and Compliance to implement and monitor this program.

2.0 Identification of red flags

In the course of managing care for patients, CBHM/CHIPA may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. The following have been identified as potential red flags.

- 2.1 A complaint or question from a patient based on the patient’s receipt of:
  - 2.1.1 A bill for another individual
  - 2.1.2 A bill for a product or service that the patient denies receiving;
  - 2.1.3 A bill from a health care provider that the patient never patronized; or
  - 2.1.4 A notice of insurance benefits (or explanation of benefits) for health care services never received
- 2.2 Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
- 2.3 A complaint or question from a patient about the receipt of a collection notice from a bill collector.
- 2.4 A patient or health insurer reports that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
- 2.5 A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
- 2.6 A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

**Comprehensive Behavioral Health Management/College Health IPA  
Policy and Procedure Manual**

|  |  |
|--|--|
| <b>Policy Name:</b> Identity Theft Prevention  | <b>Security of Personal Health Information</b>     |
| <b>Date:</b> 07-09<br><b>Reviewed by QI Committee:</b> 07-09, 11-09<br><b>Revised by QI Committee:</b> 11-09 | <b>Page:</b> 2 of 3<br><b>Policy Number:</b> SC-11 |

- 2.7 A patient who has an insurance number but never produces and insurance card or other physical documentation of insurance.
- 2.8 A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud agency.

3.0 Detect Red Flags

CBHM/CHIPA staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. CBHM/CHIPA will verify patient identity, address, and insurance coverage at the time of patient contact. Reference AR-2: *“Intake and Referral”* and HP-2: *“Caller Identification.”*

- 3.1 When a patient is referred to a contracted provider’s office for the initial appointment, the provider is advised to verify patient’s identity with the following documentation
  - 3.1.1 Picture identification
  - 3.1.2 Insurance card
- 3.2 Providers are encouraged to update this identification process every six months.
- 3.3 CBHM/CHIPA staff and contracted providers should be alert for the possibility of identity theft in the following situations.
  - 3.3.1 The photograph on the picture identification does not resemble the patient.
  - 3.3.2 The patient submits identification that appears to be forged.
  - 3.3.3 Identification documents have conflicting information.
  - 3.3.4 An address or telephone number is discovered to be incorrect, non-existent or fictitious.
  - 3.3.5 The patient’s signature does not match a signature in the practice records.
  - 3.3.6 The social security number or other identifying information matches another patient’s records.

4.0 Respond to Red Flags

If an employee or contracted provider of CBHM/CHIPA detects fraudulent activity or if a patient claims to be a victim of identity theft, CBHM/CHIPA will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under HIPAA security standards, SC-9: *“Incident Report”* will apply.

- 4.1 The employee should gather all documentation and report the incident to his or her immediate supervisor.
- 4.2 The supervisor will determine whether the activity is fraudulent or authentic.

**Comprehensive Behavioral Health Management/College Health IPA  
Policy and Procedure Manual**

|  |  |
|--|--|
| <b>Policy Name:</b> Identity Theft Prevention  | <b>Security of Personal Health Information</b>     |
| <b>Date:</b> 07-09<br><b>Reviewed by QI Committee:</b> 07-09, 11-09<br><b>Revised by QI Committee:</b> 11-09 | <b>Page:</b> 3 of 3<br><b>Policy Number:</b> SC-11 |

- 4.3 If the activity is determined to be fraudulent then CBHM/CHIPA should take immediate action. Actions may include:
  - 4.3.1 Cancel the transaction;
  - 4.3.2 Notify appropriate law enforcement;
  - 4.3.3 Notify the affected patient;
  - 4.3.4 Notify affected providers; and
  - 4.3.5 Assess impact to organization.
- 4.4 If a patient claims to be a victim of identity theft
  - 4.4.1 The patient should be encouraged to file a police report for identity theft if he/she has not done so already.
  - 4.4.2 CBHM/CHIPA will compare the patient's documentation with personal information in the organization's records.
  - 4.4.3 If following investigation, it appears that the patient has been a victim of identity theft, CBHM/CHIPA will promptly consider what further remedial act/notifications may be needed under the circumstances.
  - 4.4.4 The contracted provider will be advised to review the affected patient's medical record to confirm whether documentation was made in the patient's medical record that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.
  - 4.4.5 CBHM/CHIPA will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action taken. The patient is responsible for contacting ancillary service providers.
  - 4.4.6 If following the investigation, it does not appear that patient has been a victim of identity theft; CBHM/CHIPA will take whatever action it deems appropriate.