



## **Red Flag Rule - Identity Theft Prevention Policy**

Federal Law defines medical identity theft as:

“a fraud committed or attempted using the identifying information of another person without authority to obtain medical services or goods, or when someone uses the person’s identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.”

### **POLICY**

In accordance with the Identify Theft Red Flags and Address Discrepancies, through the Federal Trade Commission issued 11/1/2008 Capital Health Plan strives: 1) to prevent the intentional or inadvertent misuse of member names, identities, medical records; 2) to report criminal activity relating to identity theft and theft of services to appropriate authorities; and 3) to take steps to correct and/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

### **PURPOSE**

The Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft. The Red Flag regulations require healthcare entities to have a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft. The purpose of this policy is to set forth the guidelines for Capital Health Plan management and staff to use as an on-going effort to detect, prevent and mitigate identity theft.

### **PROCEDURE**

**A. DETECT** Capital Health Plan’s work force should report to the Compliance and Privacy Officer any triggers that may indicate possible identity theft which includes, but may not be limited to:

1. A complaint or question from a member based on the member’s receipt of
  - a. a bill for another individual;
  - b. a bill for a service that the member denies receiving;
  - c. a bill from a health care provider that the member never patronized; or
  - d. an Explanation of Benefits or other notice for health care services never received.
2. Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the member.
3. Refusal to provide requested identification, lack of identification or mismatch between recorded picture ID information and patient (person presenting for care).

4. A dispute of a bill by a member who claims to be the victim of any type of identity theft.
5. A member who never has evidence of an insurance card or who appears not to be the same person that staff recall from prior visits.
6. Multiple requests for new ID cards in the same year.
7. A notice or inquiry from an insurance fraud investigator or law enforcement agency.
8. A complaint or question to Member Services that may indicate an investigation is needed regarding possible misinterpretation or error in billing.
9. A complaint or question raised by a member which is communicated to the clinical staff regarding possible identity theft or services given to another other than the member.

**B. PREVENT AND MITIGATE** Capital Health Plan has several processes in place to protect our members:

- a. specific procedures are in place, under the HIPAA policies, based upon state and federal requirements, which allow members to review their medical record and to request amendments;
- b. the NextGen<sup>®</sup> Electronic Medical Record has a template customizable for Addendums and Modifications, including documentation in a wrong chart, inadvertent or otherwise;
- c. specific IS security policies and procedures to protect the computer applications and access management, using role based access, password, anti-spam software and encryption technologies.

**C. TRAIN AND EDUCATE** Capital Health Plan ensures staff, members and affiliate providers are aware of the RED FLAG Rules and the Identification Theft Prevention Principles at least annually or when there are changes that need to be implemented to improve the processes in place.

**D. PROGRAM ADMINISTRATION** Oversight of the program is from the Information Security Officer, Chief Information Officer and the Compliance and Privacy Officer to include: a) assignment of specific responsibility for training; b) reviewing reports prepared by staff; c) approving material changes to the program to address changing identity theft risks; and d) investigating complaints that have been reported by Member Services, Clinical staff, Patient Accounting staff, members, Network Providers, facilities or any other means of communication and take appropriate action including notification of law enforcement as well as notifying the victim when identity theft is discovered.

**Revision History**

Compliance Committee Approved Date: 6/2/2009

Reviewed Only: 5/21/2013, 8/19/2014, 8/25/2015, 5/24/2016

Revised: 11/15/2011

Policy Location (s): Compliance Intranet – Compliance Policies- CHP Website-Beacon



