
 <p>HAWAII HEALTH SYSTEMS CORPORATION "Quality Healthcare for All"</p>	<p>Quality Through Compliance</p>	<p>Procedure No.:</p> <p>CMP 0015B</p>
		<p>Revision No.:</p> <p>N/A</p>
<p>Procedure</p>	<p>Issued by:</p> <p>Chief Compliance and Privacy Officer</p>	<p>Effective Date:</p> <p>December 19, 2013</p>
<p>Subject:</p> <p>Identity Theft Prevention Program ("Red Flag")</p>	<p>Approved by:</p> <p></p> <p>Alice M. Hall HHSC Acting PCEO</p>	<p>Supersedes Policy:</p> <p>N/A</p>
		<p>Page:</p> <p>1 of 3</p>

Reviewed December 6, 2013; Next Review December 6, 2016

I. PURPOSE: To establish methods that Hawaii Health Systems Corporation (HHSC) patients, employees, contracted providers, and agents may comply with CMP 0015A (Identity Theft Prevention Program Policy ["Red Flag"]).

II. PROCEDURES:

- A. Each region or facility shall adopt an Identity Theft Prevention Program (ITPP) that furthers the following strategies:
1. Identify relevant "Red Flags" (as defined by policy CMP 0015A) for covered patient accounts and billing records;
 2. Appropriately respond to any Red Flags that are detected to prevent and mitigate identity theft; and
 3. Ensure the ITPP is updated periodically to reflect changes in risk to patients or to the safety and soundness of the medical facility.
- B. The ITPP shall include or incorporate how the region or facility will:
1. Identify covered accounts
 2. Identify relevant Red Flags
 3. Detect Red Flags
 4. Respond to Red Flags
 5. Oversee the ITPP
 6. Identify the stakeholders in the program and clearly define the roles and responsibilities of the various stakeholders in the program
 7. Train employees, vendors, and medical staff
 8. Verify patient identity at time of registration such as requesting:
 - a. Driver's license or other photo identification
 - b. Copy of current insurance card
 - c. Copy of other document showing the patient's address, e.g., utility bill
- C. The region or facility ITPP shall include a process for investigation and response to suspected identity theft, including, but not limited to:
1. Notifying affected person(s) that there has been a security breach following discovery or notification of the breach.

2. Filing a police report and completing the Federal Trade Commission ID Theft Affidavit by the suspected victim of identity theft.
 3. Asking the suspected victim of identity theft to provide:
 - a. Copies of his/her driver's license or other identification;
 - b. Documentation of the patient's residence address;
 - c. Any known facts about the identity theft;
 - d. Other related information.
 4. Stopping collection on open accounts.
 5. Isolating and correcting, upon facility verification of the subject patient's information, inaccuracies in medical records resulting from the identity theft.
 6. Placing a notation concerning the identity theft in the medical record.
 7. Removing all incorrect demographic information from the medical record.
- D. Each region or facility's ITPP shall include the necessary reporting requirements to comply with all Federal and State laws. Such reporting requirements shall include, but not be limited to:
1. Submitting a written report to the Hawaii State Legislature within 20 days after the discovery of a material occurrence of a social security number disclosure by the Facility that is prohibited by HRS Section 487N-4. The report shall contain:
 - a. Information relating to the nature of the incident;
 - b. The number of individuals affected by the incident;
 - c. Any procedures that have been implemented to prevent the incident from reoccurring.
 2. Complying, when applicable, with CMP0014A "Data Breach Response" that implements the reporting requirements of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), 45 CFR parts 160 and 164, and the Health Information Technology for Economic and Clinical Health Act (HITECH), Section 1176(b) of the Social Security Act, 42 U.S.C.1320d-5(b).

III. APPLICABILITY: These procedures shall apply to all HHSC Facilities.

IV. AUTHORITY: See HHSC POLICY CMP 0015A

V. ATTACHMENTS: None