

 <p><b>HAWAII HEALTH SYSTEMS</b> CORPORATION "Quality Healthcare For All"</p> <p><b>POLICY</b></p>	<p><b>Department:</b></p> <p>Quality through Compliance</p>	<p><b>Policy No.:</b></p> <p><b>CMP 0015A</b></p>
	<p><b>Issued by:</b></p> <p>David Lane, Ph.D., CCPO</p>	<p><b>Revision No.:</b></p> <p>1</p>
<p><b>Subject:</b></p> <p>Identity Theft Prevention Program ("Red Flag")</p>	<p><b>Approved by:</b></p> <p><i>Carol VanCamp</i> HHSC Board of Directors By: Carol A. Vancamp Its: Secretary/Treasurer</p>	<p><b>Effective Date:</b></p> <p>December 19, 2013</p>
		<p><b>Supersedes Policy:</b></p> <p>April 6, 2010</p>
		<p><b>Page:</b></p> <p>1 of 2</p>

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

**I. PURPOSE:** Each region or facility of the Hawaii Health Systems Corporation (HHSC) shall establish an Identity Theft Prevention Program (ITPP) designed to prevent or mitigate, respond to, and report identity theft

**II. DEFINITIONS:**

Identity Theft Prevention Program (ITPP). An effective ITPP addresses various indications, markers, or "Red Flags" that can alert staff or a facility that possible identity theft of individuals may be occurring.

"Red Flags" are defined as including, but not limited to, the following:

- A. Alerts, notifications, or other warnings received from consumer report agencies.
- B. Suspicious documents (e.g. obvious forgeries, photograph, misinformation, or physical description not matching person tendering information) such as:
  1. Photograph on the driver's license does not resemble the patient;
  2. Physical description on the driver's license does not match the patient's appearance;
  3. Signature on the driver's license or other documents does not match the patient's signature, and/or;
  4. The social security number or other personally identifying information furnished by the patient is not the same as identifying information in the facility records.
- C. Suspicious personally identifiable information (e.g. addresses, social security numbers, etc.) where:
  1. Information on one form of identification is inconsistent with information on another form of identification, or with information already in the facility's records, e.g., the address, phone number, etc. does not match existing records;
  2. The address given does not exist or is a P.O. Box;
  3. The social security number is invalid, as social security number must consist of three fields:
    - a. Area number (first three digits). Area numbers 666, 772, or above in the 700 series, or 800 or 900 series are invalid.
    - b. Group number (fourth and fifth digits). A group number of 00 is invalid.
    - c. Serial number (last four digits). A serial number of 0000 is invalid.

**III. POLICY:** The HHSC Board shall support the establishment and maintenance of an effective ITPP at each facility and in each region. It is the responsibility of all HHSC employees, volunteers, medical staff and vendors to support and participate in efforts to prevent and mitigate identity theft by complying with the ITPP and by identifying, reporting, and alleviating conditions and practices (“Red Flags”) that may lead to increased risk of identity theft.

- A. HHSC will post on its website, in compliance with HRS Section 487N-6, a link to the Hawaii Information Privacy & Security Council “Best Practices.”
- B. The HHSC Corporate Director of Human Resources shall submit to the Hawaii Information Privacy & Security Council an annual report on the existence and character of each personal information system added or eliminated since the agency’s previous report. The report shall be submitted by September 30 of each year (HRS Section 487N-7).
- C. The HHSC Chief Compliance and Privacy Officer, in collaboration with the Regional Compliance and Privacy Officers, and Chief Information Security Officer shall:
  - 1. Ensure and coordinate compliance with HRS Section 487J-5, and HRS Chapters 487N and 487R;
  - 2. Assist individuals who have identity theft and other privacy-related concerns;
  - 3. Coordinate provision of education and information to HHSC staff and other stakeholders on privacy and security issues;
  - 4. Coordinate with state, county, and federal law enforcement agencies on identity theft investigations, and;
  - 5. Recommend policies and practices to protect individual privacy rights relating to the individual's personal information.
- D. The Chief Information and Security Officer shall work with the HHSC Information Security Team to incorporate the policy incorporated in ITD 0132A.

**IV. APPLICABILITY:** This Policy applies to all HHSC facilities.

**V. AUTHORITY:** HRS Ch. 323F; HRS Ch. 487J; HRS Ch. 487N; HRS Ch. 487R; 45 CFR parts 160 and 164; 42 U.S.C.1320d-5(b), Section 1176 (b) ; ITD 0132A.

**VI. ATTACHMENTS:** Procedure CMP 0015B