HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Compliance	Policy No.: **CMP 0015**
		Revision No.: N/A
Policies and Procedures	Issued by: David Lane, Ph.D., CCPO; Stephen Wada Charla Ota	Effective Date: April 6, 2010
Subject: Identity Theft Prevention Program Policy ("Red Flag")	Approved by: Alice Hall, Interim PCEO Alice M. Hall	Supersedes Policy: FIN Interim
		Page: 1 of 4

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. 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.

III. DEFINITIONS:

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

IV. PROCEDURE:

A. Each region or facility shall adopt an ITPP that furthers the following strategies:
   1. Identify relevant "Red Flags" (as defined in Section III.C., below) 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 identify 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 CMP0014 "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).

V. POLICY AND OVERSIGHT RESPONSIBILITY

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 Vice President, 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, 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.

VI. Applicability

All HHSC facilities.

VI. 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)