HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Information Technology Department	Policy No.: **ITD 0011**
		Revision No.: N/A
Policy	Issued by: Dennis Sato Vice President & CIO	Effective Date: 03/01/02
Subject: ***Information Stewardship***	Approved by: Thomas M. Driskill, Jr. President & CEO	Supersedes Policy: N/A
		Page: 1 of 3

I. PURPOSE: The purpose of this policy is to delineate the roles and responsibilities of individuals whose roles encompass information resource owners, custodians, and users.

II. POLICY: This policy has been established in order to comply with Public Law 104-191, a federal law enacted on August 21, 1996, that is otherwise known as the Health Insurance Portability and Accountability Act (HIPAA).

Roles and responsibilities of individuals whose roles encompass information resource owners, custodians, and users are delineated in this policy.

A. Roles and Responsibilities of Information Resource Owners: Information Resource Owners are executive and department level management personnel. These management personnel may function as information resource owners in one or more roles with specific responsibilities as defined below:

1. Business Process Owner: Business Process Owners determine business requirements and classification levels of information resources in accordance with the Data Classification Policy (ITD 0009), they define access rules, are involved with business continuity planning efforts, and respond to audits and reviews.

2. Information Owner: Information Owners define access rules, assign appropriate security labels and markings, are involved with business continuity planning efforts, and respond to audits and reviews.

3. Application Owner: Application Owners define access rules, control domain boundaries, assign appropriate security labels and markings, are involved with business continuity planning efforts, and respond to audits and reviews.

4. Systems Owner: Systems Owners define access rules and security domains, control domain boundaries, assign appropriate security labels and markings, are involved with business continuity planning efforts, and respond to audits and reviews.

B. Roles and Responsibilities of Information Resource Custodians: Information Custodians are individuals (often staff within the Information Technology Department or departmental systems administrators) in physical or logical possession of information. At a minimum, custodians will be responsible for:

1. Administering controls to protect information from unauthorized access, alteration, or destruction.

2. Overseeing data back-up and recovery efforts to ensure the availability of information resources.

3. Performing monitoring activities to ensure that only authorized users are accessing the data resources that they are permitted to access.

4. Administering system configuration controls.

C. Roles and Responsibilities of Information Resource Users: Information Users are individuals who have been granted explicit authorization to access, modify, delete, and/or utilize information by the relevant owner. Users must:

1. Use the information only for the purposes specifically approved by the Owner.

2. Comply with all security measures defined by the Owner, and implemented by the Custodian and/or defined by policies and standards.

3. Report all situations where they believe a security violation has occurred.

D. Designating Owners: Management personnel may take on multiple data ownership roles as described in Section II. A. Owners may delegate responsibilities to others, but they will remain responsible for their fulfillment. However, Owners can not assign or delegate ownership responsibilities to contractors, consultants, or individuals in outsourcing firms or external service bureaus.

Managers in the Information Technology Department can not be Owners of any information, except for operational computer and network information.

E. Designating Custodians: Owners will assign responsibility to Custodians who will be responsible for administering data protection controls. It will be permissible for Custodians to be contractors, consultants, or individuals at outsourcing firms or external service bureaus.

F. Designating Users: Users are defined to be, but are not limited to be, all HHSC employees, including independent contractors, and physicians and healthcare providers as defined by Medicare or Medicaid programs, temporaries, consultants, or third parties with whom special arrangements (such as Business Associate Contracts or non-disclosure agreements) have been made. All Users must be known to and authorized by Owners. To allow proper privilege assignment and activity logging, Users must always be specific individuals. Users can not be defined as departments, project teams, or groups.

G. Changes in Status: If the employment status of Owners, Custodians, of Users change, it will be the responsibility of department managers to immediately notify Human Resources of changes in employment status (see ITD 0005 for details).

As specified earlier, Custodians are charged with administering user access controls. When a Custodian has a change in status, it will be the responsibility of an Owner to promptly assign a new Custodian. When an Owner has a change in status, it will be the responsibility of the Chief Information Officer to promptly designate a new Owner.

III. REFERENCES/RELATED POLICIES

- ITD 0009 - Data Classification Policy
- ITD 0005 - Information Systems Access Policy

IV. POLICY DEVELOPMENT

DEVELOPERS: HRC Policy Committee
Taylor Summers
Miles Sato, CISSP

V. POLICY APPROVAL

VI. REVIEWS

Revision 02/08/2002