

|   |   |                                       |
|---|---|---------------------------------------|
|  <p><b>HAWAII HEALTH SYSTEMS</b><br/>C O R P O R A T I O N<br/><i>"Touching Lives Everyday"</i></p> <p><b>Policy</b></p> | <b>Department:</b><br>Information Technology<br>Department            | <b>Policy No.:</b><br><b>ITD 0004</b> |
|   | <b>Issued by:</b><br>Barbara Kahana<br>Vice President & CIO           | <b>Revision No.:</b><br>1             |
| <b>Subject:</b><br><b><i>Information Security</i></b>   | <b>Approved by:</b><br><br>Thomas M. Driskill, Jr.<br>President & CEO | <b>Effective Date:</b><br>10/04/04    |
|   |   | <b>Supersedes Policy:</b><br>03/01/02 |
|   |   | <b>Page:</b><br>1 of 2                |

- I. **PURPOSE:** This policy establishes the rationale for the development and promulgation of IT security policies. It is based on external auditor recommendations, final HIPAA security rule requirements, and generally acknowledged IT best practices.

The final HIPAA security rule specifically mandates that HHSC must:

- Ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI).
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
- Protect against any reasonably anticipated uses or disclosures of ePHI that are permitted or required under the final HIPAA privacy rule.
- Ensure workforce compliance with the provisions set forth in the final HIPAA security rule. Compliance with the final HIPAA security rule is mandated by federal statute.

- II. **POLICY:** Reasonable and appropriate policies and procedures shall be developed and implemented to comply with the mandates promulgated by the final HIPAA security rule.

These policies and procedures must be maintained in written or electronic form, and must be retained for a minimum of 6 years from the date of their creation, or the date when they were last in effect, whichever is later.

Periodic review is required, and updates must be performed as needed in response to environmental or operational changes that may affect the security of ePHI.

Reasonable and appropriate policies and procedures shall also be developed and implemented to comply with all other applicable State and federal laws, rules, and regulations, which may encompass forms of protected health information other than in electronic form.

**III. SCOPE:** This policy applies to all forms of information, including computer and network systems owned by and/or administered by HHSC. Similarly, this policy applies to all platforms (operating systems), all computer types (personal computers, including PDAs, such as, Palm Pilots, and mainframe systems), and all application systems (whether developed in-house or purchased from third parties).

#### **IV. RESPONSIBILITIES**

**A. Responsibility of Every Worker:** To be effective, information security must be a team effort involving the participation and support of every HHSC worker who deals with information and/or information systems. Every worker at HHSC -- no matter what their status (employee, contractor, consultant, temporary, volunteer, student, etc.) – must comply with HHSC information security policies.

**B. Assigned Security Responsibility:** The Corporate Information Security Officer (CISO) is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. The CISO is responsible for compliance checking to ensure that organizational units are operating in a manner consistent with these requirements and investigations of system intrusions and other information security incidents. Violations of information security requirements will be addressed by local managers working in conjunction with the CISO and the Human Resources Department.

#### **V. DEFINITIONS**

- **Confidentiality:** Ensures that information is accessible only to those authorized to have access.
- **Integrity:** Safeguards the accuracy and completeness of information and processing methods.
- **Availability:** Ensures that authorized users have access to information and associated assets when required.
- **HIPAA:** 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).