HAWAII HEALTH SYSTEMS CORPORATION "Quality Healthcare For All"	Department: Information Technology Department (ITD)	Policy No.: ITD 0051A
		Revision No.:
POLICY	Issued by: Privacy and Security Council	Effective Date: October 17, 2013
Subject: *Information Security*	Approved by: Carol VanCamp HHSC Board of Directors By: Carol A. VanCamp Its: Secretary/Treasurer	Supersedes Policy: N/A
		Page: 1 of 7

Last Review: 05/08/2013; Next Review: 05/08/2014

I. PURPOSE:

The purpose of this document is to define corporate policy regarding the confidentiality, integrity and availability of information regardless of the location or type and to provide guidelines for stakeholders using this information. It also provides to HHSC Management the direction and support for information security in accordance with business requirements and relevant laws and regulations.

II. DEFINITIONS:

Term	Definition
Access Control	The management of admission to or use of system and network resources. Granting authenticated user access to specific resources based on company policies and the permission level assigned to the user.
Business Owner	An individual who is familiar with an application or other asset and its use in a facility, department or business unit. Typically, this is a senior or mid-level manager in that facility or department or business unit who can address requirements concerning availability and functionality of the application.
Incident / Security Incident	Events that take place on any HHSC information system that violate the confidentiality, integrity, or availability of the system and/or its data.
Information Assets	All resources such as data centers, communications rooms, databases and other data repositories, servers, workstations, handheld computing devices, networking infrastructure, routers and other communications hardware, disk drives, etc. that form a system that is used to maintain and process information that is needed to allow HHSC to perform its mission.

Information Owner	Management representative of the organization who reviews and authorizes access to or release of information that is under his/her stewardship, and is responsible for its accuracy, integrity, and timeliness.
Security Contact	HHSC employee designated to facilitate account creation, modification, and deactivation for facility or department stakeholders
Stakeholders	Any person who uses HHSC Information Assets, including, but not limited to HHSC facility and corporate office employees, board members, volunteers, students, physicians, vendors, contractors, and other external parties.
System Administrator	Individual performing system administration activities such as monitoring security configuration, managing allocation of user names and passwords, monitoring disk space and other resource use, performing backups, and setting up new hardware and software. Often with role designated as "admin", "sysadmin", "site admin".

III. POLICY:

1. Philosophy

HHSC believes that information is vital to its mission to provide high quality patient care, and to that end, HHSC needs to use information effectively while protecting the information from unauthorized or inappropriate use. Data in all forms (electronic, paper or other) throughout its life cycle (creation, storage, access, reproduction, transmission, distribution, and destruction) must be protected from unauthorized access, modification, disclosure or destruction, whether accidental or intentional. HHSC has the responsibility to protect individual patients, care providers, researchers and other parties that provide or use the information.

2. Information Security Policy Framework

HHSC has adopted the International Organization of Standards (ISO) Codes of Practice for information security management as its framework for information security policies which defines how these policies are to be implemented. HHSC will periodically review and update security policies to reflect changes in the ISO codes of practice.

All HHSC information security documentation including, but not limited to, policies, standards and procedures, must be classified as “Internal Use Only,” unless expressly created for external business processes or partners.

HHSC must employ industry-specific information security standards that are reviewed periodically to insure they are consistent with current best practices. HHSC will employ a policy-driven information systems security architecture approach that takes into consideration HHSC’s business goals and objectives. The implementation will be coordinated and managed by the HHSC Information Security Team. The Team is managed by the Chief Information Security Officer (CISO) with oversight from the HHSC Privacy and Security Council.

3. **Protection and Use of Information**
HHSC Information Assets must be consistently protected in a manner commensurate with their sensitivity, value, and criticality. Information is a critical and vital asset, and all information will be accessed, used, transmitted, reproduced and stored in a manner that provides the maximum amount of protection from inappropriate disclosure while permitting efficient operation and professional conduct of HHSC business.

4. **Stakeholder Accountability and Responsibility**
It is the responsibility of each stakeholder to be familiar with and follow this policy. Each stakeholder should know how to protect information and how to gain access to information needed to perform job duties or functions. Each stakeholder should be aware that there are various HHSC confidentiality and information security policies available to assist in understanding and supporting this policy. If a stakeholder is assigned a logon ID and password for access to electronic information, the stakeholder shall be responsible not to disclose the password to anyone.

The viewing, printing, downloading or transmitting of obscene or objectionable material on the Internet or through e-mail is strictly prohibited. Stakeholders should recognize that violation of these policies will be subject to corrective action up to and including termination of employment, in accordance with applicable collective bargaining agreements and Human Resources policies and processes. In some cases, violation of these policies might subject an individual to criminal prosecution and/or reporting to a licensing board.

5. **Systems Protection and Activity Monitoring**
HHSC uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by its computers and communications systems. In keeping with these objectives, HHSC maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. HHSC is not responsible for loss or damage to data or software that results from its efforts to meet these security objectives.

No one may willfully attempt to degrade the performance of or deny access to HHSC Information Assets, use loopholes in computer security systems or knowledge of a special password to damage HHSC Information Assets, obtain extra resources from another user, gain access to systems or accounts, or use systems or accounts for which proper authorization has not been granted.

HHSC has the right to monitor individual user activity on its Information Assets, including computer systems, telephone systems, voice mail systems, Internet activity, e-mail and other confidential information traffic at any time. Monitoring may be conducted on any basis, including routine, random or triggered by particular events or usage. Monitoring shall be conducted when there is evidence of any user activity which is prohibited, violates HHSC policy, or might jeopardize the normal operation of the Information Assets. HHSC monitoring of individual communications may be reviewed and approved by HHSC Executive Leadership or its designee. Non-enforcement of any policy requirement does not constitute waiver or consent by HHSC.

6. **Policy Conflicts and Exceptions**
HHSC Information Security Policies were drafted to meet or exceed the protections found in existing laws and regulations. Any HHSC Information Security Policy believed to be in conflict with existing laws or regulations shall be promptly reported to the CISO.

These policies are intended to supplement rather than supersede existing HHSC policies and procedures. In case of a conflict, the CISO should be notified and will work with the applicable stakeholders to resolve the conflict.

Exceptions to information security policies are permissible only in those instances where a risk assessment examining the implications of noncompliance has been performed and the CISO has approved and documented the exception.

7. **Compliance with Legislative, Regulatory and Contractual Requirements.**
HHSC will comply with the security requirements governing electronic information as denoted in the Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, as amended by Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, Pub.L. 111-5, 123 Stat. 226, February 17, 2009, and their implementing regulations at 45 C.F.R. 160 and 164, as amended from time to time (collectively referred to as "HIPAA"), and other federal and state laws and regulations governing electronic security, as they are enacted or amended from time to time. The HIPAA Administrative Information Security Standard sets forth the minimum requirements for compliance, and all stakeholders are encouraged to exceed these minimal standards. All HHSC Information Owners and HHSC Managers are responsible for reviewing these laws and ensuring that they are applied in their areas of responsibility. HHSC Management will consider prosecution for known violations of the law.

8. **Rights of Stakeholders**
It is the policy of HHSC to respect and maintain the confidentiality of patients, business partners, employees, and other stakeholders. Refer to HHSC Policy # CMP019A – HIPAA "Minimum Necessary" Standard Compliance.

9. **Audit and Security Controls**
HHSC Information Owners are responsible for defining a method of auditing their respective systems to ensure compliance with the information classification policy (ITD 0072 Information Classification Policy) and its guidelines. Information Technology Department is responsible for developing an effective system to monitor access to the overall network, and to individual components as necessary. Periodic checks should be made in all work areas to ensure that employees are aware of and complying with information security policies. All information systems security controls must be technically and operationally feasible and have a way to evaluate their alignment with existing security policies prior to being adopted as a part of standard operating procedures.

10. **Security Education, Training and Awareness Requirements**
All stakeholders will be provided training on their individual responsibilities regarding information security and the definition thereof. All stakeholders are hereby advised that HHSC Information Security Policies are available on the HHSC Intranet. All stakeholders will receive a copy of this policy and a HHSC Privacy and Security

Handbook. This documentation will be provided to new stakeholders during their initial orientation. Following initial orientation, stakeholders shall complete information security awareness training as outlined in the table below. Additionally, Managers shall orient new stakeholders to any facilities, Corporate Office or department-specific security procedures, and shall include information security and confidentiality in the annual performance review process for employees.

Stakeholder	Method and Frequency	Responsible Party
Physicians employed by HHSC, and Board Members	Initial orientation	New Employee Orientation and responsible manager
Physicians not directly employed by HHSC	Initial Confidentiality Acknowledgement and periodic renewal. Pre-education training as necessary for access to HHSC Information Assets	Responsible Manager
Volunteers	Initial orientation, and periodic training if appropriate	Responsible Manager
Contractors	Initial orientation, and periodic training if term is > 1 year	Responsible Manager
Employees, Management, and ITD Staff	Initial orientation and periodic on-line training	New Employee Orientation and responsible manager

11. Incident Reporting

All stakeholders are responsible for complying with the HHSC Information Security Policy. It is the responsibility of all stakeholders to report violations or suspected violations of this policy to their Manager or to the CISO. All incident reports relating to information security will be maintained by Corporate Compliance in order to assure the confidentiality of the document.

Users are responsible for:

- Using HHSC Information Assets for the purposes intended.
- Promoting awareness and use of applicable security controls as defined by policies and procedures.
- Complying with custodian-established controls and backup procedures.
- Reporting the loss or misuse of HHSC Information Assets promptly to the CISO, Corporate Compliance and Privacy Officer, or their Manager.

12. Business Continuity & Disaster Recovery Management

Designated Information Owners are responsible for assessing the potential impact that loss of information would have on HHSC business activities. The impact analysis along with provisions for business continuity and risk assessment should be updated periodically and on kept file with the HHSC Information Security Team. A Disaster

Recovery Plan (DRP) shall be maintained on the HHSC Intranet by HHSC Information Security Team and HHSC Corporate and Regional Management under the oversight of the CISO. The plans should include provisions for continuity of facility or department business operations and recovery in the event of disaster. Details for recovering critical information via backup and recovery operations will be included in the plan

13. Review of Information Security Policy

The Information Security Policy shall be reviewed periodically and when significant changes occur, in order to ensure its continuing suitability, adequacy and effectiveness. The review shall include feedback from relevant HHSC stakeholders at Corporate and Regions, with results of independent reviews and recommendations by management and relevant authorities. Changes in policy shall be in response to changes in the HHSC environment, business circumstances, legal conditions or technical environment. A copy of the policy will be maintained on the HHSC Intranet for easy access by stakeholders.

The Privacy and Security Council is an appointed committee that recommends changes in policy, provides oversight for the program and approves exceptions to the HHSC Information Security Policy. A cross section of HHSC personnel is assigned to this committee. The committee meets at least quarterly in conjunction with the Corporate Compliance Committee and is advisory to the HHSC Administration and HHSC Board of Directors. The CISO will serve as the ITD information security staff contact for the committee. Refer to HHSC Policy # CMP021A – Privacy and Security Council.

IV. RESPONSIBILITIES:

HHSC Executive Leadership shall be accountable for the operation of a successful, compliant information security program.

HHSC Management shall be accountable for the ownership of information and responsible for ensuring that adequate resources are in place for information security administration, including classification, criticality, access and disclosure, and risk analysis.

The HHSC Information Security Team is responsible for working with HHSC Management on overall development, implementation, maintenance and updating of information security policies and procedures; and providing support for information security in accordance with business requirements and relevant laws and regulations.

Information Owners, Business Owners, Security Contacts, and System Administrators are responsible for implementing, monitoring and issuing access codes, ensuring access authorization, defining access control profiles, monitoring system security and integrity and performing contingency planning activities. The User Provisioning Team shall be responsible for creating unique user ID's, establishing one-time passwords that must be changed by the user at initial login and granting the appropriate level of access to data per the request of the Information Owners.

Stakeholders shall be responsible for preserving the confidentiality, integrity and availability of information at the user level, complying with all HHSC Information Security Standards and ITD Policies, and reporting any security violations.

V. OWNERSHIP:

The CISO is responsible for all updates to the policy document. This document shall be reviewed and/or updated yearly. Change requests to this policy must be submitted in writing to the CISO. Please contact the CISO for questions or updates to this policy.

VI. APPLICABILITY:

This policy applies to all HHSC facilities and HHSC Corporate Office stakeholders. Compliance with this policy is mandatory. Compliance will include periodic reviews by the HHSC Information Security Team. Information Security Policy Exception Requests must be submitted in writing by relevant Management to the CISO, who will facilitate HHSC Leadership review and approval. Requests shall include justification and benefits attributed to such exception.

VII. AUTHORITY:

- ISO/IEC 27002:2005, an information security standard published by the International Organization for Standardization (ISO) and by the International Electro technical Commission (IEC), entitled Information technology - Security techniques - Code of practice for information security management:
    - Section 5: Security Policy Management Objectives
        - 5.1 Establish an information security policy
- 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)
- Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, Pub.L. 111-5, 123 Stat. 226, February 17, 2009
- 45 C.F.R. 160 and 164, as amended
- 45 CFR 164.308(a)(1)(i)

VIII. ATTACHMENTS: N/A