HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Information Technology Department	Policy No.: **ITD 0024**
		Revision No.: 1
Policy	Issued by: Barbara Kahana Vice President & CIO	Effective Date: 09/12/06
Subject: ***Wireless***	Approved by:	Supersedes Policy: 09/01/02
	Thomas M. Driskill, Jr. President & CEO	Page: 1 of 2

I. PURPOSE: This policy establishes requirements for eligible employees and physicians who have a direct need for wireless access to HHSC information systems for business purposes. It is based on external auditor recommendations, final HIPAA security rule requirements, and generally acknowledged IT best practices.

II. POLICY: All installations of 802.11 wireless network Access Points (APs) must be approved by IT management prior to APs being physically connected to the HHSC network. Wireless connectivity to the HHSC network shall be approved when at a minimum all of the following criteria are met and validated by IT management:

- Business drivers should be identified prior to enabling wireless technology.
- This policy follows the recommendations from the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS) information security standards.
- Information broadcast from any wireless device to an authorized AP must conform to the IEEE 802.11i (WPA2) wireless security standard. Advanced Encryption Standards (AES) will be utilized to encrypt data. A management approved IEEE 802.1x Extensible Authentication Protocol (EAP) shall be utilized for authentication (refer to HHSC standards list).
- Broadcasting of AP service set ID's (SSID's) must be disabled.
- CM Forms will be used to request and modify the configuration of AP's. The Technical Services Department (TSD) will configure all Wireless Access Points (AP) prior to deployment as well as modify configuration after deployment.
- The Regional IT will be responsible for granting access, accounting for user access to meet Information Access Policy (ITD-0005) requirements, monitoring their use through HHSC's central monitoring system and reporting irregularities.

- Default simple network management protocol (SNMP) community string values must not be used.

- Prior to installation the Regional IT staff must verify with the facilities Biomedical department that the wireless equipment will not interfere with any medical equipment.

- In compliance with the HHSC Certification/Internal Audit Policy (ITD0013), the security staff will coordinate periodic wireless access point sweeps throughout HHSC facilities to search for unauthorized AP's connected to the HHSC network

III. **SCOPE:** This policy applies to all implementations of wireless connectivity to the HHSC network.

IV. **RESPONSIBILITIES:** IT management shall be responsible for approving AP connections to the HHSC network, and for ensuring that the minimum wireless security provisions outlined in this policy are met. The security staff shall be responsible for coordinating periodic wireless access point sweeps throughout HHSC to ensure that no unauthorized AP's are connected to the HHSC network, and will perform periodic audits to ensure compliance with the provisions enumerated in this policy.

V. DEFINITION

- **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).

VI. REFERENCES/RELATED POLICIES

- ITD 0013 - Certification/Internal Audit
- ITD 0005 – Information Access
- National Institute of Standards and Technology (NIST) 800-43
- Federal Information Processing Standards Codes
- BS ISO/IEC 17799:2005