HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Information Technology Department	Policy No.: **ITD 0032**
		Revision No.: N/A
Policy	Issued by: Barbara Kahana Vice President & CIO	Effective Date: 5/30/07
Subject: ***Blackberry Use***	Approved by: Thomas M. Driskill, Jr. President & CEO	Supersedes Policy:
		Page: 1 of 2

I. PURPOSE:

The purpose of this policy is to define the standards, procedures, and restrictions for the procurement and ongoing use of Blackberry devices intended for use with HHSC's networked resources. This policy addresses all of the components that make up Blackberry "support" at HHSC, including (but may not be limited to):

- BlackBerry-branded and/or licensed handhelds.
- BlackBerry Enterprise Server software.
- BlackBerry Desktop Manager software.
- Wireless voice services associated with BlackBerry devices.
- Any related components of network infrastructure used to provide connectivity to the above.
- Any third-party hardware, software, processes, or services used to provide connectivity to the above.

The policy applies to any BlackBerry and/or Research In Motion (RIM)-manufactured or licensed hardware and software that could be used to access HHSC resources.
The goal of this policy is to manage the use of HHSC resources in a secure and cost effective manner while protecting HHSC systems and data from unauthorized use or exposure.

II. POLICY:

1. It is the responsibility of any HHSC staff user who is connecting to the HHSC's network via a BlackBerry-branded device or service to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection, including, but not limited to BlackBerry-class devices and service, used to conduct HHSC business be utilized appropriately, responsibly, and ethically. Blackberry users are subject to The HHSC's security policies.

2. Employees using BlackBerry-branded devices and services for remote wireless access will, without exception, use secure remote access procedures. This will be enforced through strong passwords in accordance with the HHSC's password policy. Faculty and/or staff users agree to never disclose their passwords to anyone.

3. All BlackBerry-branded equipment and devices used for business interests must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried.

4. Prior to initial use or connecting to the HHSC's network, all BlackBerry-branded and licensed hardware, software and related services must be registered with Information Services. No HHSC employees or contractors will make modifications of any kind to HHSC-owned and installed wireless hardware or software without the express approval of Information Services. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

5. The BlackBerry-based wireless access user agrees to immediately report to his/her manager and the HHSC's Information Services department if the device is lost or stolen, any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

6. Information Services reserves the right to turn off without notice any access to the network that puts the company's systems, data, users, and clients at risk.

7. Any questions relating to this policy should be directed to:

Taylor Summers, Corporate Information Systems Security Officer, (808) 933-0648 tsummers@hhsc.org

III. SCOPE:

This policy applies to all HHSC workforce members that are currently using, or wish to use, BlackBerry-based technology to access the HHSC's data and networks via wireless means.
All new hardware, software, and/or related components that provide BlackBerry-related connectivity and services for HHSC users will be managed by Information Services. The installation and/or use of BlackBerry-related hardware, software, and/or related components not approved by Information Services, are not allowed. In order to provide reliable and secure service, Information Services will support and provide access and email redirection from the Blackberry Enterprise Server. Desktop redirection is not supported or allowed.
This policy is complementary to any previously implemented policies dealing specifically with network access, wireless access, and remote access to the enterprise network.

ELIGIBLE USERS

All HHSC workforce members requesting a BlackBerry device or BlackBerry services that will be paid for with HHSC funds must go through an approval process. The individual must outline the job related need and what level of service the employee is requesting and their Manager must approve the request.
HHSC staff may not use privately owned BlackBerry-branded equipment for business purposes. The IS department cannot and will not provide technical support for third-party wireless hardware or software, or any other unapproved remote e-mail connectivity solution.

IV. RESPONSIBILITIES:

. Executive management and Department Managers are responsible for approving the use of BlackBerry devices for business purposes. IT will be responsible for supporting and maintaining HHSC owned BlackBerry devices.

V. REFERENCES/RELATED POLICIES

- ITD 0012 Password Policy, ITD 0017 Electronic Mail Policy, and ITD 0006 Remote Access
- 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)