HAWAII HEALTH SYSTEMS CORPORATION **Policy**	**Department:** Information Technology Department	**Policy No.:** **ITD 0032A**
		Revision No.: 1
	Issued by: Alan Ito Chief Information Officer	**Effective Date:** June 21, 2012
Subject: ***Mobile Device Use***	**Approved by:** Carol VanCamp HHSC Board of Directors By: Carol VanCamp Its: Secretary/Treasurer	**Supersedes Policy:** ITD 0032 (May 30, 2007)
		Page: 1 of 4

Last review: February 7, 2012; Next review: February 7, 2015

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

- BlackBerry-branded and/or licensed handhelds, BlackBerry Enterprise Server software, or BlackBerry Desktop Manager software
- IOS (iPhone/iPad) or Android-based mobile devices (smartphones or tablets)
- Mobile Device Management (MDM) Enterprise Server software, which is required for all IOS or Android-based mobile devices
- Wireless voice services associated with mobile 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 mobile device 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 mobile 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, IOS, or Android-based devices and services, used to conduct HHSC business be utilized appropriately, responsibly, and ethically. Mobile device users are subject to the HHSC's security policies.

2. Employees using mobile 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. In addition, all IOS and Android-based mobile devices are required to use MDM for HHSC messaging and calendaring.

3. All mobile 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. All users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jail breaking" or "rooting" your iPhone or Android device. You may lose the ability to communicate with the HHSC network should your device undergo such a change in configuration.

4. Prior to initial use or connecting to the HHSC's network, all mobile device 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 mobile device 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. Users may not connect a mobile device to the HHSC infrastructure without documented consent from HHSC Information Services. HHSC Information Services reserves the right to disable or disconnect some or all services without prior notification.

8. Any questions relating to this policy should be directed to: James Brady, PhD, Chief Information Security Officer, (808) 733-4090, jbrady@hhsc.org

III. SCOPE:

HHSC is structured as a single corporation and assets are confined to a single Information Systems Network Infrastructure. As such, the protection of HHSC's information systems infrastructure (consisting of hardware, software, networks, communications, data, facilities, human resources, and services) must be protected uniformly by all Regions. The IT Security Policies are developed to protect all assets confidentiality, integrity, and availability system wide and also comply with Federal, State, and other regulatory laws. Therefore, the HHSC Corporate Board of Directors must have oversight of Security policy approval and support required adherence to the policies.

This policy applies to all HHSC workforce members that are currently using, or wish to use, mobile device-based technology to access the HHSC's data and networks via wireless means. All new hardware, software, and/or related components that provide mobile device-related connectivity and services for HHSC users will be managed by Information Services. The installation and/or use of mobile device-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 or Mobile Device Manager 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 mobile device or mobile device 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 use privately owned Apple IOS (iPhone/iPad) or Android mobile devices, provided Mobile Device Management software is used on these devices to access HHSC email and calendaring data. 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.

HHSC RELEASE OF LIABILITY AND DISCLAIMER TO USERS OF PERSONAL MOBILE DEVICES

Mobile device users hereby acknowledge that the use of personal mobile devices in connection with HHSC business carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, in addition to programming errors that have the potential to render a device inoperable. HHSC hereby disclaims liability for the loss of any such data and/or for service interruptions. HHSC expressly reserves the right to wipe Blackberry devices, or IOS/Android-based devices using the MDM application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining the HHSC service. Furthermore, depending on the applicable data plan, the software may increase applicable rates.

IV. RESPONSIBILITIES:

HHSC management is responsible for approving the use of mobile devices for business purposes. IT will be responsible for supporting and maintaining HHSC-owned mobile devices. For non-HHSC-owned IOS and Android-based mobile devices, IT will be responsible for supporting and maintaining the MDM application, while the user will be responsible for all other aspects of the mobile device, including hardware, non-MDM software/applications, and voice and data plan costs.

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)