
Department: UW Medicine Information Technology Services

Policy Number: SEC-05.06 PDA and Smart Phone Usage in the UW Medicine Environment: Minimum Information Security Standard

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

The purpose of this standard is to document UW Medicine minimum requirements for all PDA's that may use any of UW Medicine's networks, and document proper security procedures.

Standard

The technology to secure PDAs and Smart Phones is not yet mature and there are significant risks associated with using these devices to store and/or transmit sensitive data. It is UW Medicine policy that any PDA or Smart Phone used to store and/or transmit sensitive information be equipped with appropriate security features.

- I. **Standard for all PDAs and Smart Phones.** All PDAs or Smart Phones used to conduct UW Medicine¹ business or are used on the UW Medicine network must meet the following minimum requirements:
 - Updated and patched operating system.
 - Password protected.
 - Ability to disable the wireless port if you do not use wireless transmissions.
- II. **Standard for PDAs and Smart Phones used to store/transmit sensitive information.** All PDAs or Smart Phones using UW Medicine Protected Health Information (PHI)or storing passwords, are required to have the following minimum security features:
 - Active network filtering or a firewall.
 - No automatic login. Configure the OS to prevent automatic log in.

¹ For the purposes of HIPAA, UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; Hall Health Primary Care Center; University of Washington Physicians; UW Medicine Eastside Specialty Center, as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.

- Encryption function for storing PHI and/or passwords.

III. Additional security recommendations for PDAs and Smart Phones used to store/transmit sensitive information. It is recommended that all individuals who use PDAs and Smart Phones for storing/transmitting UW Medicine Protected Health Information or storing passwords, observe the following additional safeguards:

- Use active protection against malicious software and scan for viruses prior to connecting to the UW Medicine network. Any workstation used to synchronize PDAs should have current antivirus software installed on it;
- Do not use wireless transmissions to send or receive PHI or passwords on your PDA or Smart Phone unless you are using an approved Virtual Private Network (VPN);
- If multiple users share a PDA or Smart Phone - each user needs their own loginID & password;
- Use automatic bit wiping software, which wipes your device clean after too many failed log-ons or if the PDA isn't hot-synced within a specified time;
- To increase chances a lost PDA will be returned; Password protect it so no one else can use it, then put your phone number in a visible location on the outside of the device and keep a business card in your PDA case;
- Record serial numbers and passwords for software separate from your PDA in case you need to reload;
- Put your PDA in an electronic shielding bag to prevent wireless transmission leakage.

UW Medicine IT Services: _____ Date: _____

James S. Fine, M.D., CIO, ISO