University of Wisconsin School of Medicine and Public Health
Department of Family Medicine Personal Digital Assistant Policy

1.0 Policy Name

Department of Family Medicine Personal Digital Assistant (PDA) Policy

2.0 Definition and Purpose

This policy outlines the following information:

- Expected employee behavior regarding the use of Personal Digital Assistants (PDAs), which often contain sensitive data such as Protected Health Information (PHI), stored passwords and sensitive departmental information.
- Supported devices and levels of connectivity allowed.
- Service and support levels from DFM ITS staff.
- Outlines and information on reimbursements for devices and device services.

2.1. Definition of a PDA

a. For the purpose of this policy, a PDA is defined as any of the following devices:
   1) Blackberry hand-held devices
   2) Apple iPhone Devices
   3) Apple iPod Touch Devices
   4) Apple iPad Devices

3.0 Scope of Policy

This policy applies to all PDAs, whether DFM or employee owned. These include but are not limited to:

- Devices used for business purposes such as the storage of PHI, passwords or sensitive departmental information.
- Any device that connects to or accesses a DFM, UWMF, or UW resource such as email, system calendars or file systems.
- Any device provided by DFM as part of a technology pilot or test program.

4.0 Policy Statement

4.1. Level of Support

a. Supported Hardware

1) DFM ITS supports Apple iTouch, iPad or iPhone (3.0s or above) and BlackBerry (4.5 or above) mobile devices. A list of specifications and recommended devices can be found at https://inside.fammed.wisc.edu/administration/its/pda
No other devices are supported.

b. Supported Software

The DFM ITS department supports a variety of software on mobile devices. This list changes periodically. DFM ITS will review new software and requests for inclusion in this list on a regular basis. Please see the address below for a current list of supported software.

1. https://inside.fammed.wisc.edu/administration/its/pda software

c. Syncing and Backup

1) DFM ITS supports syncing BlackBerry devices wirelessly via UWMF managed services.
2) DFM ITS supports syncing Apple devices wirelessly via a DFM approved and managed system.
3) DFM ITS recommends syncing with only one computer.
4) Backup is the responsibility of the DFM employee. PDAs should be backed up regularly to prevent data loss.
5) DFM ITS will coordinate a sync location at work upon request.

d. Mobile Access to DFM Systems

1) Non-Apple Devices
    I. Mobile access to GroupWise is available from the UWMF for Palm OS, Windows Mobile OS, BlackBerry, and Symbian OS devices. BlackBerry OS devices are preferred.
2) Apple Devices
    I. Mobile access to GroupWise is supported by DFM ITS staff via a DFM approved and managed system.
3) Support for mobile access is limited to providing the connectivity, and does not include support for configuring the device. Configuring connectivity is the responsibility of the user and should be done with the assistance of the service provider.
4) Eligibility for mobile connectivity access is determined on an individual basis.
5) Employees using mobile connectivity from the UWMF must adhere to the UWMF Support Policy for Personal Desktop Assistants. This Policy is shared upon request of the service.
6) BlackBerry devices have additional costs consisting of approximately $80 in setup costs and $30 per year, which will be incurred by the employee's budget unit or paid with the requesting employee's CME funds.
7) Apple devices have additional costs consisting of approximately $100 in setup costs, which will be incurred by the employee's budget unit or paid with the requesting employee's CME funds.
8) To request Blackberry mobile access, please send an email to atgheat@uwhealth.org, and a ticket will be generated.
9) To request Apple mobile access, please see the DFM web site at http://addresstocomelater.com.

e. Priority

1) PDA support is notoriously time intensive. Therefore, all requests for support will be treated as medium priority. Exceptions can be made on a case by case basis.

4.2 Registration of PDAs

a. All PDAs used for business purposes, either DFM or employee owned, must be registered with DFM ITS. Mandatory registration is a part of the DFM HIPPA compliance efforts.
b. It is the responsibility of the DFM employee to register the PDA by contacting DFM ITS.
c. DFM ITS will provide an asset sticker to place on the back of a PDA. The sticker provides a DFM ITS phone number in the event the PDA device is lost.

4.3 Power-on Password

a. All PDAs are required to have a power-on password.
b. Power-on password must be at least four characters long, not contain more than two identical characters and cannot include a character sequence (e.g. 1234, ABCD).
c. The auto-lock feature should be set in accordance with best practices.
d. No attempt should be made to circumvent or change the required security settings.

4.4 Protected Health Information (PHI)

Users have a responsibility to understand and adhere to DFM policies guiding the secure use of PDA devices. Specifically, any user of a PDA containing PHI agrees that no attempt will be made to circumvent any security mechanisms or security software placed on this device for the purpose of bypassing the required authentication procedures.

a. All PDAs used to store PHI or confidential information must use encryption or additional PDA security software that has been approved by DFM ITS to protect data confidentiality.
b. PDAs that store PHI data must be registered with the DFM ITS**.**
c. During the PDA registration process, employees will be given instructions regarding the installation process for the additional PDA encryption software.
d. It is the responsibility of DFM employee storing PHI and/or passwords on an unapproved device (Windows Mobile, Palm, Android, etc.) to ensure that the device adheres to the same security standards as outlined in this document for DFM supported PDAs.
e. Employee will follow strong password guidelines as stated in Employee Technology Security Policy for encryption software if PHI is stored on PDA.
    1) Passwords are required to be a minimum of eight characters.
    2) Passwords must have at least one numeric character, one punctuation character, and one uppercase alpha character.
    3) Passwords should not be a word found in the dictionary, in any language, slang, jargon or a name.

f. PHI may not be stored on removable memory cards.
g. Prior to an Employee or Guest or a resident leaving DFM, PHI must be removed from PDA.
h. If an Employee or Guest sells or donates a PDA containing PHI, the Employee or Guest must ensure the removal of PHI.
i. Contact DFM ITS staff for additional information or assistance about PDA technical support and/or PDA security issues.

4.5 PDA Disposal/Repair/Replacement

A PDA that is discarded, upgraded, replaced or returned to manufacturer must, if possible, be reset to the original factory configuration prior to the device leaving control of the DFM employee. If this is not possible, then all data must be removed from the device. DFM employees are strongly encouraged to contact the DFM ITS group for assistance with this process to ensure HIPAA compliance.

4.6 Lost, Stolen or Damaged Devices

Any device purchased with DFM/UW/UWMF funds is the property of the organization and not of the employee. As such, employees must return devices to the organization when they are not longer employed. As a part of the registration process of a new device, the DFM will provision all devices to protect against dissemination of PHI or other confidential information through Remote Wipe capabilities. This capability allows DFM ITS staff to remotely issue a command to a lost or stolen device to erase all information on the device. Any DFM employee requesting access to DFM resources through a PDA understands and agrees to the following:

a. The DFM has the right to Remote Wipe any device it suspects has been compromised, lost, or stolen.
b. Employees agree to notify DFM ITS staff as soon as possible that a device has been lost or stolen. This notification will occur via a phone call (or in extreme circumstances an email).
c. Employees understand that data backup is the responsibility of the user and DFM is not liable for any personal information lost as a result of a Remote Wipe.
d. If the device is recovered, DFM ITS will assist the user in restoring all DFM-specific applications and restoring resource access. Restoration of personal information is the responsibility of the user.
e. Employee agrees to treat the device in an appropriate manner and to guard against damage and destruction whenever possible.
f. Employees found to frequently damage, destroy or misuse devices owned by the organization may be subject to disciplinary action. DFM reserves the right to remove any device from an employee at any time.

4.7 CME funded purchases

Employees with CME funds may use those funds to purchase a PDA device as outlined by this policy. Purchases must be approved by the employee's manager/supervisor and meet the specifications outlined in the policy.

a. Purchases of Apple iPad devices must be coordinated with DFM ITS staff. ITS will purchase the device, coordinate appropriate billing and perform initial configuration of the device.
b. Purchases of other (non-iPad) devices should be coordinated with the employee's department administration and DFM Finance.

5.0 Effective Date of Policy

This policy was approved on 7/26/2010.

6.0 Policy Review

This policy will be reviewed on an annual basis by ITS staff and DFM Administrative Leadership.