University of Wisconsin
School of Medicine and Public Health
Department Family Medicine
Employee or Guest Technology Security Policy

---

1. Policy Name

Department Family Medicine (DFM) Employee or Guest Technology Security Policy

2. Definition and Purpose

This policy outlines expected employee or guest behavior regarding the use of technology resources and methods for accessing/storing Protected Health Information (PHI) in accordance with HIPAA Privacy Policy, HIPAA Security Policy, and UW-Madison Appropriate Use Statement. The policy applies to employees or guests using DFM technology resources. Guests are defined as consultants, auditors, students and/or anyone using DFM technology resources beyond a visiting presenter.

3. Reference to HIPAA Standard

Security Management Process (161.308(a)(1)); Information Access Management (161.308(a)(4)); Security Awareness and Training (161.308(a)(5)); Access Control (161.312(a)); Person or Entity Authentication (164.312(d)).

4. Scope of Policy

This policy applies to Department of Family Medicine employees or guests utilizing technology resources owned and operated by the Department of Family Medicine**.**

5. Policy Statement

5.1 Computer Standards

Employees/guests are responsible for adhering to the Computer Support and Standards Policy.

5.2 Disposal of PHI

a. Disposal of electronic PHI includes hard drives, USB external memory device, CD-R/RW, floppy disks, zip disks and any other type of media that can store electronic PHI data.
b. Acceptable methods for the disposal of electronic PHI include magnetic degaussing, overwriting data with a series of characters or pulverizing media.
c. Once a desktop and/or laptop has been determined to be at the end of its life cycle, the desktop and/or laptop must be returned to the DFM Helpdesk to undergo the appropriate level of data disposal.
d. Employees/guests are expected to seek assistance from the DFM Helpdesk or appropriate clinic Information Services staff member regarding the appropriate disposal of electronic PHI data.

5.3 Email Use

a. Passwords must not be inserted into email messages or other forms of electronic communication unless protected by encryption.
b. Remote access to email is available via GroupWise WebAccess
c. DFM email accounts cannot be forwarded to a third-party email provider outside of the .wisc.edu domain.
d. Employee/guests are expected to exercise due caution when opening any attachments.
e. If an employee or guest suspects a workstation/laptop has been infected with virus, the employee/guest should contact the DFM Helpdesk or appropriate clinic Information Services staff.
f. Patients must provide written consent for patient-to-provider email. The consent form is to be stored with patient records. Refer to consent form at https://inside.fammed.wisc.edu/documents/3139
g. PHI (Protected Health Information) may be sent via email to recipients within the .wisc.edu domain. However, employees/guests should exercise due caution to include only the

minimum necessary amount of PHI AND to de-identify the PHI so that personal identifiable information is not included in the email.

h. PHI should not be included in an emails sent to mailing lists.
i. The above steps are stop-gap measures to provide due diligence in regards to PHI and email until such time when UW Health has identified and adopted further measures for protecting the confidentiality and integrity of email containing PHI.

5.4 Home Computer Usage

a. PHI is not to be stored on a home personal computer.
b. If an employee/guest uses a personal home computer to access any UW-Madison or UW Health technology resource, the employee/guest must install and maintain current anti-virus software. A free version of anti-virus software can be obtained from DFM Helpdesk.
c. The following software recommendations are recommended for home computer use to reduce security risk:
    1) Operating system automatic updates
    2) Firewall
    3) Anti-Spyware

5.5 Installing Software

a. Employees/guests are not to install software. This includes, but is not limited to, downloading games, wallpaper, weather notifications, and/or file sharing services.
c. To request software installations, employees/guests can contact the DFM Helpdesk or contact the appropriate clinic Information Services staff.

5.6 Laptop Appropriate Use

Employees/guests are responsible for adhering to the Laptop Appropriate Use Policy.

5.7 Leave Workstation Powered On To Receive Critical Updates

a. Employees/guests are to leave their workstation powered on overnight to automatically receive critical software updates.

5.8 Moving Equipment

a. Computers/WinTerms/Printers at all DFM work facilities are tracked to a specific location and to a specific employee/guest for inventory, auditing, security and operational purposes.
b. Due to Epic work flow, it is required that workstations/printers/WinTerms moves be coordinated between DFM ITS and UWMF. Contact the DFM Help Desk for further instructions.

5.9 Passwords

a. UW Health (Novell, GroupWise, Metaframe, Epic) passwords will expire every 90 days.
b. Passwords are required to be a minimum of eight characters.
c. Passwords must have at least one numeric character, one punctuation character, and one uppercase alpha character.
d. Temporary passwords must be changed after the first use.
e. Passwords must not be shared. In rare cases where a password needs to be shared, DFM Helpdesk or the appropriate ITS staff member must be consulted to ensure appropriate restrictions are in place for the protection of data.
f. At no time can passwords providing access to PHI be shared. This includes, but is not restricted to PHI applications such as, Epic, RECIN, WISCR-IT, and Practice Partner.
g. Passwords should not be a word found in the dictionary, in any language, slang, jargon or a name.

    For example, create a phrase that has special meaning, and add punctuation and a numeric value.

    Passphrase: Green Bay won superbowl=96!
    Password; GBws=96!

h. It is the responsibility of the employee/guest to police and monitor the secure storage of passwords and to safeguard passwords in the same manner as keys. Passwords are not to be stored under keyboards, on monitor, etc.

i. Passwords can be securely stored on a PDA with the use of approved encryption software. For more information regarding the secure storage of passwords, please contact the DFM Helpdesk.
j. Employees/guests should not use the "Remember Password" feature found in applications.
l. Password and system audits will be performed on a periodic basis to assess risk levels. If during an audit a password is determined to be a risk, the employee/guest will be required to change password.
m. If an employee/guest suspects that someone has accessed his/her account, the employee or guest should contact the DFM Helpdesk.

5.10 PDA Security

Employees/guests are responsible for adhering to the PDA Security Policy and PDA Support Standards.

5.11 PHI (Protected Health Information)

a. DFM Employees/guests must complete the online HIPAA training at: ~~http://ptehipaa.doit.wisc.edu/moodle/login/index.php~~ (Policy currently under review.)
b. DFM Employees/guests must store PHI on a server, such as Novell file server.
c. Access to PHI requires a unique username and password.
d. PHI cannot be stored on workstation/laptop hard drive, Personal Digital Assistant (PDA), nor portable media device without use of encryption software approved by DFM ITS**.**
e. Laptops and/or PDAs that store electronic PHI data must be registered with the DFM Helpdesk.

5.12 Portable Media & PHI

a. PHI is not to be stored on portable media such as floppies, CD-RW, USB key fobs, Zip disks.
b. In the exception where PHI does need to be stored on a portable media device, the employee or guest must use encryption software that has been approved by the DFM ITS.

5.13 Social Engineering

a. Employees/guests are not to give out account information to any unsolicited caller or person. A common technique among hackers/crackers is to try and lull an employee or guest into giving out account information such as login ID or password for unauthorized access.
b. While working in the teaching clinics, DFM ITS staff will be identified by an identification badge or a nametag.
c. Report suspect activity regarding the use of technology resources to DFM Helpdesk. Suspect activity might include unknown person(s) requesting passwords, repeated account lockouts, or an unknown person(s) working on your workstation.

5.14 Use of Fax Machines, Printers, Copy Machines

a. Fax machines and printers that routinely receive transmission of electronic PHI shall be placed in a secure, non-public area. Public areas inappropriate for the location of Fax machines and printers include, but are not limited to, primary hallways, waiting rooms, multi-use and conference rooms and/or elevator lobbies.
b. A fax cover sheet that includes a confidentiality statement shall be used as a cover page when faxing PHI.
c. Copy machines should be attended during the copying of PHI.
d. Employees/guests should remove PHI output from printers, fax machines, copiers as soon as possible to avoid unauthorized persons from gaining access to the materials.
e. Employees/guests should exercise care to Fax PHI contents to appropriate recipient and to verify the total number of pages received as identified on a fax cover sheet.

5.15 Use of Personally Owned Laptops/Desktops/Printers

a. Personally owned desktops/laptops/printers cannot be connected to the DFM/UWMF wired network due to security issues.
b. Computing devices (desktop/laptops/printers) that connect to a DFM/UWMF wired network must meet ALL of the following criteria:
    1. Must be purchased with DFM funds, UW Health funds, or grant funds.

2. Meet pre-approved technical specifications as designated by DFM ITS staff.
3. Be set up and configured by DFM ITS staff.

5.16 Wireless

a. Wireless networks must be approved, configured and managed by DFM ITS staff.
b. Personally owned laptops may connect to an authorized DFM public wireless network.
c. DFM ITS staff does not provide support for personally-owned wireless networks nor hot spot WIFI networks.

5.17 Workstation Screensavers

a. When leaving workstations for an extended period of time, employees/guests are expected to lock the workstation.
b. Workstations have a password-protected screensaver activated after 15 minutes of idle use.
c. Shared workstations have either a password protected screensaver activated after 15 minutes of idle use or a screen distortion device to prevent incidental access to PHI displayed on a monitor.
d. Upon request, provider workstations in private offices can be configured to have a password-protected screensaver blank at 15 minutes and require a password after an additional 45 minutes.

6. UW-Madison Responsible Use of Information Technology Policy

Guidelines for Responsible Use of University of Wisconsin-Madison Information Technology can be found here: http://www.cio.wisc.edu/policies-responsibleuse.aspx

7. Employee or guest Accountability

a. New employees/guests will receive and review this policy with a supervisor or designee appointed by the supervisor. The supervisor/designee will obtain a signature sheet from the employee/guest and return the Signature Sheet to the DFM Help Desk within two days of the employee/guest start date.

b. When a violation of a technology policy occurs, the employee's supervisor should consult with the ITS Director to determine the appropriate course of action.

c. Violations of the DFM Employee or guest Technology Security Policy may lead to the suspension of computer access privileges pending investigation of circumstance. Violations of this policy will be referred to the employee/guest's supervisor and/or DFM Human Resources. Unacceptable use of any DFM technology resource could result in penalties as severe as termination of employment and/or criminal prosecution. Depending on the offense, violators may be subject to prosecution under State and/or Federal laws.

8. Policy Review

This policy will be reviewed by the ITS Oversight Committee every two years.

Implementation Date	October 2004
Revision Date	September 2005
Revision Date	October 2007
Revision Date: updated #6	November 2011