UWMS Department of Family Medicine
DFM Email Policy

1.0 Policy Name
Department of Family Medicine Email Policy

2.0 Definition and Purpose
This document defines email usage for Department of Family Medicine employees.

3.0 Scope of Policy
This policy applies to Department of Family Medicine employees utilizing technology resources owned and operated by the Department of Family Medicine.

4.0 Policy Statement

4.1 General Use

a. Email is a primary means of communication within the department, and all employees will be given accounts and are expected to use them.

b. DFM employees may choose to use a DFM email account, another University of Wisconsin email account (such as WiscMail or UWMF mail) or an Aurora.org email account as appropriate.

c. If using DFM mail, Email addresses will be in the firstname.lastname@fammed.wisc.edu format, for example jane.doe@fammed.wisc.edu.

d. DFM email addresses may consist of letters, a period, a hyphen (-, and an at sign (@). Numbers and other punctuation, such as apostrophes, are not allowed

e. It is the employee's responsibility to insure that their email address is kept up to date and that their correspondents know their correct email address.

f. Email addresses for employees can be found by querying the directory on www.fammed.wisc.edu and in the GroupWise address book.

4.2 HIPAA Compliance

a. Use of electronic Protected Health Information (ePHI) in Emails

When including ePHI in an email Family Medicine employees are expected to:

1) Exercise extreme caution.
2) Verify recipient address.
3) When possible, de-identify ePHI such that an individual cannot be identified.
4) Use only the minimum necessary amount of ePHI needed for a related work function.

b. Patient to Provider Email Communication

Providers communicating with patients via email must have patients complete the DFM "Agreement for Using for Patient-Provider Communication."

1) The agreement form is at:http://www.fammed.wisc.edu/administration/ptconsent.pdf,
2) The agreement for patient-provider email is to be stored with patient records
3) Emails between patient-provider are to be retained in the patients' record.
4) Emails directed to a provider will be responded to within five business days.
5) Emails may be viewed/responded to by clinic staff other than the provider.

6) Patient-Provider email must not be used for urgent matters that require a response in less than five business, nor should patient-provider email be used for life threatening or serious life altering matters.
7) For more specific guidelines regarding patient-provider email, refer to http://www.fammed.wisc.edu/administration/ptconsent.pdf,

c. DFM Provider Consulting with External Provider

For the purpose of patient treatment, payment, operations purposes it is acceptable to include ePHI in an email. For the purpose of patient treatment, it is acceptable for a Family Medicine provider to include ePHI in an email to a provider at another health care organization such as GHC or Dean, etc. Encryption is not needed.

d. Recipient Within .wisc.edu Domain

If the recipient's email address ends in ".wisc.edu", it is acceptable to include ePHI in an email for the purposes of a work related function. Encryption is not needed.

e. ePHI on Email Lists

ePHI should not be included in an email sent to an email list nor to an email group.

f. Email Confidentiality Statement

Employees must have the following confidentiality statement appended to their email messages:

This email and any attachments may contain confidential information to be used only by the intended recipient(s). Email communications are not considered secure. If you are not the intended recipient(s) of this email, you are expected to disregard the content, delete the email message, and notify the original sender.

g. Future Directions

The above steps are stop-gap measures to provide due diligence in regards to use the ePHI in email until such time when UW Health has identified and adopted further unified measures for protecting the confidentiality and integrity of email containing PHI.

4.3 Access

a. From Department of Family Medicine offices, employees using a DFM email account may use the Novell GroupWise client or GroupWise WebAccess.

b. From all other locations, employees using a DFM email account must use GroupWise WebAccess.

4.4 Account Setup/Modification/Deletion

a. Requests for new email accounts and account modifications must be in writing from the appropriate clinic manger/designee/supervisor in writing.

b. DFM Email accounts for exiting employees will be deleted within three days of the employee's last day of work. Vacation time or sick leave time used after the employee's last day of employment does not extend account access.

c. Graduating resident email accounts will continue to be active for six months after graduation, after which time they will be deleted.

4.5 Forwarding

a. In the case of change of email address within the University of Wisconsin network, a temporary forward will be available to the employee's new campus account for one month. This process can be setup by contacting the Help Desk.

b. In no case shall email be forwarded to an email account outside of the University of Wisconsin network, with the exception of Aurora.org.

c. It is the employee's responsibility to notify colleagues of an email address change.

d. It is the employee's responsibility to insure that their email address is kept up to date and that their correspondents know their correct email address.

e. Email addresses for employees can be found by querying the directory on www.fammed.wisc.edu and in the GroupWise address book.

4.6 Acceptable Content

a. Departmental email is intended for departmental business only. Email usage should parallel that of University or departmental letterhead.

b. While incidental personal use of departmental email is tolerated, departmental email is not to be used for excessive personal use.

c. Examples of excessive use of departmental email include, but are not limited to, email communications regarding political affiliations, sale of personal items, running or promoting a personal business, and using departmental email account as login account for a web site of personal interest.

d. For personal email, employees need to use a non-departmental email account, such as an account from your home ISP (Internet Service Provider) or a free service, like Yahoo Mail or Hotmail.

e. Departmental email groups and listservs are to be used for work related communication. Personal business or announcements such as offering items for sale or trade are not appropriate. Departmental functions such as picnics or dinners are legitimate work related activities and an appropriate use of email groups, listservs, and email.

f. For performance reasons, large attachments such as Power Point presentations should be avoided, especially when sending messages to large groups of people or to mailing lists. If you need to share files frequently, please use other resources, such as the shared drive or consider contacting the Help Desk to put the file on the web site.

g. To prevent the spread of computer viruses, files with the following extensions are blocked on our mail servers: vbs, exe, scr, com, pif, hta, bat, and password-protected *.zip files. This list is subject to change as needed.

h. Email Etiquette
   1) Refrain from using capital letters because it comes across as shouting.
   2) Verify your email is addressed to the intended recipient.
   3) Use a descriptive subject line
   4) Use caution when selecting the "reply all" feature and be sure that you want to send an email to everyone listed in the "To:" field.
   5) Be careful and polite with your tone. Depending on the situation, email may not be the

most effective tool for communication.

6) Don't believe every cyber myth or urban legend sent to you. If you receive something that raises questions, verify if content is myth at http://www.snopes.com/ before passing contents along to others.

4.7 University of Wisconsin Appropriate Use Policy for Information Technology Resources

a. All DFM employees must follow the University of Wisconsin Appropriate Use Policy for IT Resources. This document can be found at http://www.doit.wisc.edu/security/policies/appropriate_use.asp

4.8 Implementation and Review:

Policy will be reviewed on a continual basis with a formal review once a year.

Implementation Date	October 2004
Last Reversion Date	May 2005