Guidelines for Email and Protected Health Information

Medical records and other health information that identify individuals is sensitive information that is subject to the highest level of security based on University data classification standards, and is also typically subject to a variety of state and federal regulations, including the Health Insurance Portability and Accountability Act (HIPAA). This type of information is often referred to as "Protected Health Information" or PHI.

Use of PHI in e-mails is discouraged. E-mails are always subject to some level of security risk, can be sent to the wrong address, and can be forwarded to others who should not receive them. Always exercise discretion in sending e-mails with PHI, and use alternate, and more secure, forms of communication whenever possible.

In the event you determine that e-mail of PHI is necessary, you must ensure that you meet the guidelines contained in this Appendix.

PATIENTS:

E-Mailing PHI to Patients:

E-mails to patients containing that patient's PHI should be done only if the patient has specifically agreed to such a form of communication. Check with the facility where the patient is being seen to ensure that such an agreement is in place, and that you are following any additional guidelines the facility has regarding such communications.

E-Mailing Patient PHI to Others:

PHI of patients may be e-mailed to others only in the following circumstances and subject to the following guidelines:

1. The communication is sent to another e-mail address within the University, University of Minnesota Physicians, or Fairview.
2. The communication is sent only to those who have a legitimate purpose for receiving the information (such as those involved in treatment, payment for treatment, or some type of healthcare operation, including quality assurance, peer review, training or education).
3. Only the minimum amount of PHI necessary is communicated.
4. PHI containing information about AIDS, HIV, STDs, mental health, substance abuse and developmental disabilities should not be e-mailed unless required for patient safety.
5. No auto-forwarding of e-mails containing PHI to personal e-mails is permitted.
6. The following Confidentiality Statement is included at the bottom of the e-mail [NOTE: work with your IT representative to determine if this can be included in your e-mails automatically or include it as part of your signature block]:

> The information transmitted in this e-mail is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material, including "protected health information." If you are not the intended recipient, you are hereby notified that any

review, retransmission, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please destroy and delete this message from any computer and contact us immediately by return e-mail.

NOTE: E-mailing patient PHI to others beyond the University, University of Minnesota Physicians and Fairview is not secure and is prohibited.

RESEARCH SUBJECTS:

PHI of individual research subjects should not be included in e-mails or attachments to e-mails. If you are working with de-identified information (see Administrative Procedure *De-identifying Data for Research*), that information is no longer PHI and can be e-mailed, subject to any restrictions in place from your research sponsor.

HEALTH PLAN COMMUNICATIONS:

PHI of individual health plan beneficiaries should not be included in e-mails or attachments to e-mails unless the information is being submitted by a secured transmission to a University health plan administrator or consultant. Information that indicates health plan enrollment or disenrollment status or relates to general plan management or administration is not PHI and can be e-mailed**.**

Guidelines for Use of Personal Mobile Devices for University Business Including PHI

If you want to use your personal mobile device (including smartphones and tablets) to access the University system, such as your University email or calendar, and you are part of the University Health Care Components, you will need to register the device through OIT. For more information on University Health Care Components, see "Protection of Individual Health Information by U Health Care Components" Policy.

The University requires this registration in order to ensure that University information contained or accessible through your device can be secured. See related "Appendix to Policy – Guidelines for Use of Smart Phones for University Business." Any registered device that is lost or stolen must be reported to the University as stated in the "Reporting Security Incidents and Making Notification" Policy.

Registration of devices will involve:

> Creation of a pass code for access. This pass code will help deter unauthorized access to your device. You will have the ability to create your own pass code. After a period of inactivity the pass code will have to be re-entered to access the device.
>
> Management of device in the event of loss. In the event your mobile device is lost or stolen, the University will have the ability to remove all data from your device to ensure the security of any University information contained on or accessible by your device.

To initiate the registration process, contact your IT representative.