Washington University in St. Louis

# HIPAA Privacy Procedure #17-7

Effective Date: April 14, 2003
Reviewed Date: February, 2011
Revised Date:
Scope: Radiation Oncology

**Communication of Electronic Protected Health Information by E-mail**

**********

**Policy Expectation:**

Protected Health Information (PHI) should only be shared with authorized parties, in accordance with all applicable laws, rules, regulations, and Washington University (WU) policies. The communication of PHI via e-mail requires special attention since the PHI might be transferred through unsecured lines via the Internet thus compromising security and therefore privacy of PHI.

**Why is this important?**

- Ensures that e-mail containing PHI, which can be encrypted and deciphered by the receiving party is protected from being subject to eavesdropping while crossing unsecured networks.
- Ensures that e-mail containing PHI, which cannot be sent in encrypted form is sent in limited circumstances and with specific safeguards in place as defined in this procedure.
- Failure to comply may result in WU being liable for civil or criminal penalties under HIPAA regulations.

**What do you need?**

- Copy of WU HIPAA Policy on Security Measures Required to Comply with Privacy Policies.

| Steps: | Additional Information |
|---|---|
| **1. Communication of Electronic Protected Health Information by E-mail**<br>E-mail messages containing PHI may be transmitted within WU and/or BJC networks (WUSTL, WUCON and/or CARENET) in accordance with all applicable laws, rules, regulations, and WU policies.<br><br>Due to the risk of intercepted or misdirected e-mail, Washington University strongly discourages the use of e-mail for sending PHI outside of the WU and BJC networks, particularly in instances of highly sensitive PHI, such as HIV-related or mental health information. The use of e-mail for | If the destination e-mail address ends in "..wustl.edu" or "..bjc.org", the recipient is within WU or BJC networks. You may send the message.<br><br>Sample Notice of Unsecure Network e-mail:<br><br>*"Please be aware that e-mail messages may be* |

| | |
|---|---|
| transmitting PHI should only be used when other alternatives are impractical for the situation. If a decision is made to use e-mail to send PHI then only the minimum information necessary should be contained in the message.<br><br>E-mail containing PHI, which cannot be sent in encrypted form, should only be sent in limited circumstances, and with specific safeguards in place as defined below. | *copied or intercepted in transit. By sending health information via e-mail you are accepting these risks.*<br><br>*If you are concerned about the privacy of your health information we encourage you to communicate it by either telephone or FAX. If you do not wish to have your health information sent via e-mail please contact the sender immediately."* |
| **2. Communications Between Provider and Individual:**<br><br>Use a secure e-mail system when a provider and the Individual communicate via e-mail.<br><br>Only use unencrypted e-mail with an Individual under the following guidelines when a secure e-mail system is not available:<br><br>• Use of e-mail is for patient convenience or at the request of the patient.<br>• Inform the Individual of the inherent unsecured nature of e-mail, both because of the Internet and because many Individuals use e-mail which can be accessed by others (from work where their employer will have access to their system or at home where others may have access).<br>• Clearly explain to the Individual the circumstances under which the provider will use e-mail for communication (what types of transactions can be handled by e-mail vs. phone vs. office visit; average response time to a message; what to do with urgent or emergent communications).<br>• Request that the Individual agree, either in writing or by sending an e-mail response, to accept the risks of using e-mail and accept the limitation placed by the provider.<br>• Do not include PHI in the first message to the Individual. Make it a general message that confirms the e-mail address and confirms the message is received by the Individual. | This allows for an e-mail to be sent to the patient which contains no PHI, but refers them to a secure website where his/her PHI is held.<br><br>This methodology allows the ease of mail for the Individual, keeps the provider's e-mail confidential so it cannot be shared with others and keeps all PHI secure.<br><br>**Exhibit A**, Authorization to Utilize Unencrypted E-mail to Communicate Protected Health Information.<br><br>**Caution: Notice this means placing the confidentiality statement at the beginning of the message.** |

| | |
|---|---|
| • Include at the beginning of every e-mail containing PHI a confidentiality statement which states:<br><br>*The materials in this e-mail are private and may contain Protected Health Information. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this e-mail in error, please immediately notify the sender via telephone or return e-mail.* | **Caution: Notice this means only e-mails containing PHI.** |
| **3. Communications Between Providers**<br><br>Transfer PHI by unencrypted e-mail within the secure networks of WU/BJC as outlined in the WU HIPAA Procedure, Electronic Sharing/Transmission of Data Containing Protected Health Information.<br><br>Outside of the secure networks of WU/BJC, use unencrypted e-mail only in limited circumstances, when no other more secure method of communication is available and even then only in the minimum necessary amount to ensure appropriate patient care. | **Exhibit B**, E-Mail Guidelines produced by the WU Department of Risk Management. |
| **4. Regard communications by e-mail**, which concern patient care as part of the medical record. The Washington University Department of Risk Management has practice guidelines for e-mail as well as other types of electronic communications such as websites. Those guidelines should be followed as well as the HIPAA specific guidelines. | |
| **5. Develop an audit or review process** to ensure that the process for use of e-mail containing PHI is carried out in accordance with both the WU HIPAA policies and this procedure. Periodic surveillance may be used by Information Systems to ensure compliance. | |

## Exhibit A

## AUTHORIZATION TO UTILIZE UNENCRYPTED E-MAIL TO COMMUNICATE PROTECTED HEALTH INFORMATION

Thank you for your request to communicate with me via e-mail. We want to make sure you know that e-mail communications between us are not encrypted and therefore are not secure communications. If you elect to communicate with me from your workplace computer, you also should be aware that your employer and its agents might have access to e-mail communications between us. Finally, e-mail communications may become a part of your patient medical record and be accessible to my clinical support staff as needed for our operations.

Incoming e-mail communications will be reviewed and answered as soon as possible. If you have not heard from my office with a response and are concerned we may not have received the message, please call the office during regular business hours. E-MAIL COMMUNICATION SHOULD NEVER BE USED IN THE CASE OF AN EMERGENCY OR FOR URGENT REQUESTS FOR INFORMATION.

If you agree to the foregoing terms, please indicate your acceptance by responding via e-mail that you accept the terms and conditions outlined herein.

ACCEPTED: Signature of Individual_____

Authorized E-mail of Individual: _____

Date: _____ Name of Physician: _____

**Exhibit B**
**Washington University**
**Department of Risk Management**
**E-MAIL GUIDELINES**

Computer networking has greatly expanded our ability to access and exchange information, requiring more vigilant efforts and more secure safeguards to protect confidential information.

When corresponding with each other via e-mail, dissemination may well negate any legal protection such documents might have, even if they were sent to an attorney, and may arguably constitute a breach of patient confidentiality.

We advise that you refrain from addressing quality review, confidential medical and/or claim or lawsuit related issues via e-mail. When there are such issues to be addressed, we ask that you do so through your division administrator, department head, and others in the chain of command.

**Patient/Family Communication by E-Mail**

Many patients and physicians are interested in using e-mail as a two-way communication or tool for information regarding their healthcare.

There are privacy limitations. The physician has a duty to maintain confidentiality and therefore take precautions to unauthorized viewers. E-mails from patients should not be misdirected, forwarded to a third party, or used in any marketing project.

E-mails create a record of consultation and are part of the medical record. They are discoverable, even if deleted. The wording should be objective and accurate. E-mails can facilitate decision making in that they provide effective use of pharmaceutical intervention, and assist in determining the emotional state of the patient.

Prior to using e-mail with a patient, you should discuss e-mail and obtain their written consent. The consent should contain the following information:

- Types of transactions available by e-mail, e.g. patient education, prescription refills, and appointment scheduling.
- Privacy and technology issues. Identify who in the physician's office will have access to the e-mail. If the patient is using their employer's e-mail address, their employer will have access to the e-mail. The patient and physician should exchange e-mail addresses.
- Response time and emergencies. Explain an expected turn around time (how often you review) to respond to an e-mail. Tell the patient under which circumstances they should call the office or go to an emergency department. Neither of you should use e-mail for urgent matters. Remind the patient of other forms of communication, including telephone, voice mail, facsimile and postal service.
- E-mail storage. How long the e-mail will be kept and the location.

**Miscellaneous**

Physician should send an auto message when out of town. Patients need to give permission for you to share e-mails with family members. Place a header, "This is a confidential communication."

Many patients and physicians find e-mail communication to be an efficient and effective means of communication. Both parties have an opportunity to articulate questions and responses.

**Physician Web Site**

Same considerations as above and in addition need to consider state licensing, malpractice, standard setting, disclaimer statements, and limited knowledge and history of unknown patient.
September 2001