WASHINGTON UNIVERSITY
HIPAA Privacy Policy # 7

Appropriate Methods of Communicating Protected Health Information

Statement of Policy

Washington University and its member organizations (collectively, "Washington University" or "WU") are committed to conducting business in compliance with all applicable laws, regulations, and WU policies. As part of this commitment, WU has adopted a policy to provide guidelines and instructions on the appropriate communication and handling of Protected Health Information ("PHI").

WU is committed to providing quality healthcare to Individuals. Assuring the quality of services is one of the most important responsibilities of each member of the WU Workforce. **The application of this Policy should never jeopardize safety or care of Individuals.**

Scope of Policy

This Policy addresses only general situations that commonly arise and it is not intended to be all-inclusive. How one should appropriately communicate or handle PHI will frequently depend upon the surrounding facts and circumstances. Common sense and good judgment must be applied in each case.

Policy

1) Face-to-Face Communications between WU Health Care Providers.

As a general rule, conversations concerning an Individual's PHI should only occur in the context of Treatment, Payment or Health Care Operations or when the Individual has signed an Authorization. See WU HIPAA Policy on Authorization Required to Use or Disclose Protected Health Information.

If it is necessary to discuss an Individual's PHI in other contexts, under no circumstances should an Individual's PHI be discussed in any public place or area where it might be inappropriately overheard, such as cafes, elevators, hallways or public transportation.

2) Face-to-Face Communications with Family Members, Friends or Other Non-WU Persons.

Conversations with persons involved in an Individual's care, such as family members, close personal friends, or other persons identified by the Individual, generally should occur only after the Individual has given, at a minimum, his or her verbal Authorization. For further information, see WU HIPAA Policy on Verbal/Inferred Agreement to Use or Disclose Protected Health Information.

The appropriateness of a conversation involving PHI will ordinarily depend upon the surrounding facts and circumstances. This Policy cannot address all potential situations that may arise and it is not intended to be all-inclusive. Common sense and good judgment must be applied in each case. Each member of the WU Workforce who communicates PHI in a face-to-face conversation with another person is responsible for ensuring that the communication is reasonably designed to protect the PHI to the greatest extent possible without interfering with the intended purpose of the communication. At a minimum, one should:

a) Request the identity of the person requesting the PHI
b) Determine the relationship between this person and the Individual (i.e. a health-care provider, a family member providing care, payor, etc);
c) Determine the reason for requesting the PHI (i.e. for Treatment, Payment, Health Operations, Law Enforcement, etc); and
d) "Minimum necessary" amount of PHI that may be provided. See WU HIPAA Policy on Minimum Necessary Request, Use or Disclosure of Protected Health Information.

How WU satisfies this Policy depends upon the surrounding facts and circumstances. For example, if the Individual is unable to provide his or her verbal Authorization because he or she is unconscious or unavailable, then WU may use professional judgment and experience to make reasonable inferences if it is appropriate and in the best interests of the Individual to Disclose the PHI to another person. If so, only PHI directly relevant to the person's involvement with the Individual's health care should be disclosed. For example, if an Individual brings a spouse into the doctor's office or a colleague or friend brings the Individual to the emergency room for Treatment, it is reasonable to assume, absent extenuating circumstances, that the person is involved in the Individual's care and may appropriately be given general information concerning the Individual's condition without first obtaining the Individual's written or verbal Authorization.

3) Telephone Communications.

Telephone communications concerning an Individual's PHI are governed by the same rules as those discussed above for face-to-face communications. The appropriateness of telephone communications involving PHI will ordinarily depend upon the surrounding facts and circumstances. This Policy cannot address all potential situations that may arise and it is not intended to be all-inclusive. Common sense and good judgment must be applied in each case.

WU Workforce members who communicate PHI over the telephone to another person are responsible for ensuring that the communication is reasonably designed to protect the PHI to the greatest extent possible without interfering with the intended purpose of the communication. At a minimum, WU should:

a) request the identity of the person requesting the PHI;
b) determine the relationship between this person and the Individual (i.e., a health-care provider, a family member providing care, etc.);
c) determine the reason for requesting the PHI (i.e., for Treatment, Payment, Healthcare Operations, etc.); and
d) unless the PHI is being provided for Treatment purposes, decide what is the "minimum necessary" amount of PHI that may be provided. See WU HIPAA Policy on Minimum Necessary Request, Use or Disclosure of Protected Health Information.

How WU satisfies the above procedure depends upon the surrounding facts and circumstances. For example, in some cases an employee may be familiar with the identity of the caller through voice recognition. In other cases, the employee may have to use a "call-back" procedure. It may be sufficient if the caller can provide the Patient Registration Number or Patient Account Number of the bill or account they are discussing in some situations. With extremely sensitive PHI and in non-emergency situations, seeking an Authorization from the Individual should be the first option considered.

4) Facsimile Communications.

Facsimile communications are subject to the same rules as those discussed above for face-to-face communications and telephone communications. The appropriateness of facsimile communications of PHI will also depend upon the surrounding facts and circumstances. Common sense and good judgment must be applied in each case. As with telephone conversations, each member of the WU Workforce who communicates PHI over a facsimile machine is responsible for ensuring that the communication is reasonably designed to protect the PHI to the greatest extent practicable without interfering with the intended purpose of the communication. At a minimum, WU should:

a) request the identity of the person requesting the facsimile containing the PHI;
b) confirm that the facsimile number is correct;
c) do not use PHI on the cover sheet
d) determine the relationship between this person and the Individual (i.e., a health-care provider, a family member providing care, etc.);
e) determine the reason for requesting the PHI (i.e., for Treatment, Payment, Healthcare Operations, etc.); and
f) unless the PHI is being provided for Treatment purposes, decide what is the "minimum necessary" amount of PHI that may be provided. See WU HIPAA Policy on Minimum Necessary Request, Use or Disclosure of Protected Health Information.

How WU satisfies the above procedure depends upon the surrounding facts and circumstances. In some cases, an employee may (a) require a written request for a facsimile, (b) require confirmation that the receiving machine is in a secure location not accessible to unauthorized individuals, or (c) send an initial test fax to confirm the number.

PHI containing medical information or material that is normally treated with a higher level of sensitivity (i.e., HIV, Hepatitis, abortion, drug/alcohol dependence, etc.) should not be faxed unless it is absolutely necessary to facilitate an urgent need for the information due to current patient Treatment issues.

A cover sheet should accompany every electronic communication which contains the following information:

The materials enclosed with this facsimile transmission are private and confidential and are the property of the sender. 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 telecopied information is strictly prohibited. If you have received this facsimile transmission in error, please immediately notify the sender via telephone to arrange for return of the forwarded documents to us.

5)Electronic Communication between Providers and Patients

The transmission of PHI by any means of electronic communication must meet the HIPAA Security Rule requirements for the transmission of electronic protected health information.

For provider to patient communication, the Washington University Follow My Health Patient Portal is preferred over email. The patient portal allows for secure messaging between patient and provider in accordance with the HIPAA Security Rule requirements. This methodology allows the ease of email for the patient, keeps the provider's email confidential so it cannot be shared with non-patients, and keeps all PHI secure. Communication that occurs within the Washington University Follow My Health Patient Portal can easily be integrated into the patient's medical record.

Only if the patient has specifically requested email communication and has signed the Email Consent Form, may a provider may use unencrypted email with a patient. The guidelines below must be followed by the provider:

- Use of email should be for patient convenience and at the patient's request only
- The patient must be informed of the inherent unsecured nature of email, both because of the internet and because many patients use email 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).

- The circumstances under which the provider will use email for communication must be made clear to the patient (what types of transactions can be handled by email vs. phone vs. office visit; average response time to a message; what to do with urgent or emergent communications).

- The patient must agree, either in writing or by sending an email response, to accept the risks of using email and accept the limitations placed by the provider. (See **Exhibit A** for sample language)

- The first message sent to a patient should NOT include PHI, but should be a general message that confirms the email address and the patient's receipt of the message.

- In addition, for all email concerning patient care, the provider needs to treat email communications as part of the medical record. The Washington University Department of Risk Management has practice guidelines for email as well as other types of electronic communications such as websites. Those guidelines (attached in **Exhibit B**) should be followed as well as the HIPAA specific guidelines.

- Every email sent which contains PHI must have a confidentiality statement which states:

> The materials in this email are private and may contain Protected Healthcare 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 email in error, please immediately notify the sender via telephone or return email.

6) E-Mail, Internet, Electronic, Wireless or Satellite Communications.

The transmission of PHI by e-mail, by internet, or by any other means of electronic, wireless or satellite communication must meet the HIPAA Security Rule requirements secure transmission of electronic protected health information. All email containing protected health information that travels across external networks must utilize an encryption mechanism to ensure the integrity and confidentiality of the protected health information. It is the user's responsibility to ensure that protected health information is sent via email only when absolutely necessary and the message contains only the minimum amount of protected health information required.

WU workforce members should, at a minimum:

a) request the identity of the person requesting or receiving the PHI;
b) determine the relationship between this person and the Individual (i.e., a health-care provider, a family member providing care, a payer, etc.);
c) determine the reason for requesting or receiving the PHI (i.e., for Treatment, Payment, Healthcare Operations, etc.);
d) and unless the PHI is being provided for Treatment purposes, decide what is the "minimum necessary" amount of PHI that may be provided. See WU HIPAA Policy on Minimum Necessary Request, Use or Disclosure of Protected Health Information.
e) do not use patient name or other identifiers in the subject line

PHI containing medical information or material that is normally treated with a higher level of sensitivity (i.e., HIV, Hepatitis, abortion, drug/alcohol dependence, etc.) should not be electronically transmitted unless it is absolutely necessary to facilitate an urgent need for the information due to current patient Treatment issues.

For provider to provider communications, outside of the WU/BJC networks, providers will need to utilize an encryption mechanism to ensure the confidentiality of the data being transmitted. Workforce members are responsible to password protect and encrypt attachments (Word, Excel, Adobe PDF, etc.) containing protected health information prior to sending and to validate the recipients e-mail address.

In addition, for all email with outside providers concerning patient care, the provider needs to treat email communications as part of the medical record. The Washington University Department of Risk Management has practice guidelines for email as well as other types of electronic communications such as websites. Those guidelines (attached in **Exhibit B**) should be followed as well as the HIPAA specific guidelines.

Every email sent which contains PHI must have a confidentiality statement which states:

> The materials in this email are private and may contain Protected Healthcare 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 email in error, please immediately notify the sender via telephone or return email.

Creation Date: November 22, 2002
Effective Date: April 14, 2003
Last Revision Date: May 18, 2010; March 14, 2013

EXHIBIT A

AUTHORIZATION TO UTILIZE UNENCRYPTED EMAIL TO COMMUNICATE PROTECTED HEALTH INFORMATION

Electronic mail, or email, is a form of communication that may be utilized between you and the providers. We want to make sure you know that email communications between us are not encrypted and therefore are not secure communications. If you elect to communicate from your workplace computer, you also should be aware that your employer and its agents may have access to email communications between us. Finally, email communications may become a part of your patient medical record and be accessible to my clinical support staff as needed for our operations.

Incoming email communications will be reviewed and answered as soon as possible. If you have not heard from your provider's office with a response and are concerned that your message was not received, please call the office during regular business hours. EMAIL COMMUNICATION SHOULD NEVER BE USED IN THE CASE OF AN EMERGENCY OR FOR URGENT REQUESTS FOR INFORMATION.

This authorization may be revoked at any time and must be done in writing. It is understood that the revocation will not apply to information that has already been released based on this authorization.

Authorization is valid while in treatment relationship with any of the Washington University providers or in the event of:
_____.

If you agree to the foregoing terms, please indicate your acceptance by your signature that you accept the terms and conditions outlined herein.

ACCEPTED: Signature of Individual_____Date_____

Printed Patient Name _____ DOB ____/_____/_____

Authorized E-mail of Individual _____

Department of origination of authorization_____

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, i.e., patient education, prescription refills, 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 turnaround 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