UNIVERSITY OF PITTSBURGH POLICY 07-02-09

CATEGORY: PERSONNEL
SECTION: Confidentiality of Medical Information
SUBJECT: Proper Handling of Protected Health Information Outside of the University
EFFECTIVE DATE: September 23, 2013
PAGE(S): 3

I. SCOPE

This Policy applies to all University employees.

II. POLICY

It is the policy of the University to ensure that protected health information (PHI) remains confidential and secure when PHI is either provided outside of the University (for example, via email or facsimile) or when transported off University premises.

III. PURPOSE

To establish guidelines designed to protect the confidentiality and security of PHI when located or transported outside of the University in accordance with and consistent with applicable state and federal regulations.

IV. DEFINITIONS

PHI includes any known information about a patient or individual. PHI includes, but is not limited to, demographic information (such as name, DOB, age, etc.) and specific health information (such as diagnosis, history, medications, etc.)

Secured Container: A type of case or carrier that reasonably secures the information (e.g., a locked briefcase, a lidded box, a sealed envelope or other suitable carrier).

V. GUIDELINES

1. Transporting PHI Off Site

PHI should be taken off-site only if absolutely necessary for job related reasons. The person removing the information shall take all necessary precautions to protect and safeguard the PHI at all times while in their possession. This includes never leaving the PHI unattended even if in a locked vehicle. While off-site, the PHI will be the sole responsibility of the individual who removed it from the premises. The PHI should be returned to the University Covered Component as soon as possible.

When PHI is taken off site of University premises, the individual taking it off site must do so in a Secured Container.

Label the Secured Container as follows: (1) Contents property of the University of Pittsburgh, (2) Number X of X (do this even if there is just one container), (3) If found, please return to _____ (name of Covered Component, contact person and address) and (4) Confidential Information. The Attachment to this policy is a template of a label that can be used to meet this requirement.

2. Emailing PHI Outside of the University

If necessary to send an email containing PHI outside of the University, the following precautions are to be taken:

a. Wherever possible, use the University's secure e-mail service.

b. If the emailing of the PHI is not for purposes of treatment, payment or health care operations, make sure there exists a patient or individual signed HIPAA compliant authorization form in place.

c. Avoid using patient identifiers in the subject line of the email.

d. Prior to sending the email, verify the recipient's correct email address.

e. Include the following footer:

This email contains confidential information of the sending organization. Any unauthorized or improper disclosure, copying, distribution or use of the contents of this e-mail and, if applicable, attached document(s) is prohibited. The information contained in this e-mail and attached document(s) is intended only for the personal and confidential use of the recipient(s) named above. If you have received this communication in error, please notify the sender immediately by e-mail and delete the original e-mail and attached document(s).

3. Use of Mobile Devices

When using mobile devices such as a Blackberry, iPhone, iPad, or any "smart phone," etc. precautions should be taken to ensure that recommended security settings are applied to the device in order to further protect and safeguard PHI.

4. Use of Laptops/Removable Devices/Storage

If the data being stored is not encrypted by the application, then the laptop or removable device must be encrypted. In addition the device should be enabled with password protection or used with some other form of authentication such as biometrics or a token.

5. Faxing PHI Outside of the University

If necessary and appropriate to fax PHI outside of the University, the following precautions are to be taken:

a. If the faxing of the PHI is not for purposes of treatment, payment or health care operations, make sure there exists a patient/individual signed HIPAA compliant authorization form in place.

b. Use the standard University fax cover sheet. This fax cover sheet contains the necessary confidentiality disclaimer.

c. Always verify the recipient's contact information and fax number prior to faxing.

d. When faxing to non-routine locations or locations known to be in public areas, advise the recipient prior to faxing so it can be immediately retrieved. Follow-up with the recipient to verify receipt of the fax.

e. Immediately remove the PHI from the fax machine.

f. Return to the owner any PHI left on a fax machine.

g. Destroy or return to the owner any PHI received in error and advise the sender of the error.

h. Periodically verify the accuracy of pre-programmed fax numbers.

VI. NON-COMPLIANCE

An employee's failure to abide by this policy may result in disciplinary action up to and including termination of employment.

VII. REFERENCES

Attachment A – Label for Secured Container