UNIVERSITY OF PITTSBURGH POLICY 07-02-01

CATEGORY: PERSONNEL
SECTION: Confidentiality of Medical Information
SUBJECT: Privacy of Medical Records – Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
EFFECTIVE DATE: Revised September 23, 2013
PAGE(S): 3

I. SCOPE

This policy sets forth the framework for the University's compliance with the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the HIPAA Omnibus Rule. It is applicable only to those units of the University that have been designated as "Covered Components" under HIPAA. This policy is limited to the privacy standards imposed by HIPAA. Other aspects of the law, including rules governing security and human subject research, are addressed in other University policies. See the University's IRB website for policies governing human subject research.

II. POLICY

It is the policy of the University of Pittsburgh to comply with HIPAA, HITECH and the Omnibus Rule. Only designated units, departments or Schools of the University that are health care providers, health plans or health care clearinghouses which engage in electronic billing or other administrative activities related to health care operations as well as units which conduct administrative support functions for them, such as the Office of General Counsel, Internal Audit, the Office of Human Resources, Computing Services and Systems Development and the Office of Risk Management, are subject to the HIPAA regulations ("Covered Components"). This policy addresses primarily the HIPAA Privacy Rule which was effective April 14, 2003, as amended. Each Covered Component within the University is responsible for adopting site specific policies and procedures consistent with this policy.

III. HIPAA

HIPAA is a federal law that, among other things, focuses on protecting the privacy of personal health information ("protected health information" or "PHI"). This law affords certain rights to Individuals regarding their PHI and imposes obligations upon many institutions that maintain such PHI. At the University, the following components are designated as Covered Components and are responsible for compliance with HIPAA privacy regulations: the School of Dental Medicine, the University Medical and Health Plans, the Student Health Service, and the University Counseling Center, as well as workforce members of other University offices that, while offering support to these components, access PHI. These offices are the Office of General Counsel, Internal Audit, Office of Human Resources, Computing Services and Systems Development, and the Office of Risk Management. Members of the workforce of the above components must receive HIPAA training from their component. The following serve as basic reminders of key HIPAA privacy principles:

- Receive, use, and disclose PHI for purposes of treatment, payment, and healthcare operations. If you are using or disclosing PHI for purposes other than treatment, payment, or healthcare operations, please consult as necessary with the University's Privacy Officer or the Office of General Counsel to determine whether and under what conditions such use or disclosure is permissible and if HIPAA accounting rules apply.

- Adopt reasonable measures to protect PHI from unauthorized access, use, or disclosure. In considering what is reasonable, you should consider the extent to which paper records are kept in locked files or rooms; whether destruction of paper records is effective (shredding is recommended); the extent to which electronic records are accessible to unauthorized individuals; and other factors that may influence risk of unauthorized access.

- Limit the amount of information you receive, use, and disclose to what is reasonably necessary for you to do your job. Take an extra few minutes to consider whether you can reduce the amount of health information involved.

- Evaluate your agreements with vendors - especially those with access to our PHI or who create PHI on our behalf - and determine whether HIPAA Business Associate language is required for those contracts. If you have any questions on whether such language is required, or to obtain a copy of the required language, consult the University's Privacy Officer of the Office of General Counsel.

- If you have any questions, or believe that a violation of privacy has occurred, please contact the University's Privacy Officer or the Office of General Counsel as soon as possible.

IV. GUIDELINES

The HIPAA Privacy Rule requires the University to put into place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information (PHI), which is created or received by the University's Covered Components. Protected Health Information (PHI) includes any health information relating to past, present or future physical or mental health, health care treatment, or payment for health care. PHI includes information that can identify an Individual, such as name, social security number, address, date of birth, medical history or medical record number and includes such information transmitted or maintained in any format, including paper and electronic records, but excluding certain education and student treatment records. Not included within PHI are student education records, including medical records (which are protected under the Buckley Amendment), medical records of employees received by the University in its capacity as an employer, and workers' compensation records. There are special provisions in the law governing the release of psychotherapy records.

HIPAA further imposes on Covered Components of the University the following obligations:

- To notify patients, prospective, current and former faculty, staff, students and covered dependents (Individuals) about their privacy rights and how their health information can be used or disclosed.
- To adopt and implement privacy procedures for its Covered Components.
- To train employees so that they understand the privacy rules.
- To designate a Privacy Officer.
- To secure Individual records containing individually identifiable health information so that they are not readily accessible to those who do not need to see them.
- To make reasonable efforts to limit the use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose.
- To adopt special procedures for the use of PHI for research. See the University's IRB website for related policies.
- To comply with HIPAA restrictions on activities related to fund-raising and marketing.

V. SANCTIONS

It shall be the responsibility of each Covered Component to implement procedures to meet the requirements of HIPAA as set forth in this policy. Every employee in a Covered Component with

access to protected health information is required to adhere to all HIPAA mandates. Violation of this policy may result in disciplinary action up to and including termination of employment. Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties and criminal sanctions including fines and imprisonment.

VI. ADDITIONAL INFORMATION

For additional information about this Policy, contact the University's Privacy Officer, 132 Cathedral of Learning, Pittsburgh, PA 15260, by telephone at 412-624-2202, or the Office of General Counsel, 1710 Cathedral of Learning, Pittsburgh, PA 15260, by telephone at 412-624-5674.