

UNIVERSITY OF PITTSBURGH

POLICY

SUBJECT: Privacy of Medical Records – Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

DATE: April 14, 2003

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). 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 the Health Insurance Portability and Accountability Act of 1996 (HIPAA). 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 functions for them, such as the Office of General Counsel, Internal Audit and Human Resources, are subject to the HIPAA regulations. This policy addresses primarily the HIPAA Privacy Rule which is effective April 14, 2003. Final regulations for the HIPAA Security Rule have been issued and will be implemented prior to their effective date. Each covered component within the University is responsible for adopting site specific policies and procedures consistent with this policy.

III. 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 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 patient 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.

IV. 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 unit/department or School 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 of up to \$250,000 per year and criminal sanctions including fines and imprisonment.

V. ADDITIONAL INFORMATION

For additional information about this Policy, contact the University's Privacy Officer, Vice Provost Robert F. Pack, 809 Cathedral of Learning, Pittsburgh, PA, 15260, by telephone at 412-624-4228 or by e-mail at robert.pack@pitt.edu.