DRAFT – For University public comment period.

To comment on this draft Procedure, please click here.

University of Pittsburgh
Health Insurance Portability and Accountability Act
Procedure AO [insert #]

Implementing Executive: Senior Vice Chancellor and Chief Legal Officer
Responsible Unit: Office of Compliance, Investigations, and Ethics
Category: Administration & Operations
Effective Date: [insert]

I. Purpose

This Procedure defines the University of Pittsburgh's ("University") processes for administering compliance with the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 and effectuates the standards established in University Policy AO [insert #], HIPAA.

II. Definitions

Please refer to Policy AO [insert #], HIPAA, for definitions of the terms used in this Procedure.

III. Procedures

The Procedures below provide detail on:

- Privacy of Protected Health Information ("PHI") and Electronic PHI ("EPHI") (Section III. A.)
- Security of PHI and EPHI (Section III. B.)
- Use and Disclosure of PHI for Fundraising and Marketing (Section III. C.)
- Accounting of Disclosures of PHI (Section III. D.)
- Amendments to PHI (Section III. E.)
- Visitor Observation of Patients and PHI (Section III. F.)

A. Privacy of PHI and EPHI

The University's Privacy Officer shall oversee all ongoing activities related to the development, implementation, and adherence with the University's HIPAA compliance program.

Each Covered Component shall designate a component specific privacy officer and security official. The University's Privacy Officer, Chief Information Security Officer, Covered Component security officials, and Covered Component privacy officers shall work collaboratively to ensure University HIPAA compliance.

B. Security of PHI and EPHI

As noted in Policy AO [insert #], each Covered Component within the University is responsible for adhering to the HIPAA Security Rule. All University Covered Components, in coordination with Pitt IT Security, shall perform annual technical security assessments of potential risks and vulnerabilities related to the confidentiality, integrity, and availability of EPHI. On an ongoing basis, all Covered Components shall review system activity records including audit logs, access reports, security incident tracking reports, and perform annual compliance reviews. Results of the review shall be provided to the Covered Component's management, the University's Chief Information Security Officer, and the University's Privacy Officer.

Each Covered Component shall identify a security official responsible for the adherence to Policy AO [insert #] who will provide a documented response, including remediation steps for any lapses in compliance. The University's HIPAA Security Officer shall receive periodic security updates.

Each Covered Component shall establish procedures that ensure only authorized individuals access systems that manage EPHI and that systems that manage EPHI have authorization controls. Each user shall be given the minimum level of access or permissions needed to perform their job functions. Covered Components are only permitted to store, process, or transmit EPHI using devices, applications, and services approved by Pitt IT Security. Procedures shall also govern the receipt and removal of hardware and electronic media that contain EPHI.

All Covered Components shall have procedures in place for the notification of the component level security official in the event that a system managing EPHI is involved in a security incident. The security official shall follow the University's data incident response plan in terms of subsequent notification and responding to the security incident.

All Covered Components shall have a business continuity plan outlining how a component will continue operating during an unplanned disruption in service and how it will respond to emergencies that may damage systems managing EPHI.

C. Accounting of Disclosures of PHI

The University's Covered Components shall track disclosures of PHI.

A sample use and disclosure tracking form is available upon request from the Office of Compliance, Investigations, and Ethics. Please contact: compliance@pitt.edu .

The University's Covered Components shall upon written request, provide to individuals an accounting of all disclosures of an individual's PHI for up to a six-year period prior to the date

of the request. Disclosures of electronic health records shall be provided for a three-year period prior to the date of the request.

A sample request form is available upon request from the Office of Compliance, Investigations, and Ethics. Please contact: compliance@pitt.edu .

In the event of a privacy or security incident or breach, the University's Covered Components shall notify the University's Privacy Officer, the Office of Compliance, Investigations, and Ethics, and follow the University's incident response plan where appropriate.

The Office of Compliance, Investigations, and Ethics shall maintain a list of all HIPAA business associates so that individuals may contact the business associate directly to request an accounting of the business associate's uses and disclosures of the individuals' electronic health record.

The accounting shall be made in writing within sixty days of receipt of the request. One thirty-day extension is permitted per request. The content of the accounting shall include: (a) disclosures of PHI; (b) date of disclosure; (c) name of the person or entity who received the PHI; (d) the address (if known) of the entity or person; (e) a description of the PHI disclosed; and (f) a statement of the purpose of the disclosure.

D. Amendments to PHI

An individual may request, in writing, an amendment to their PHI maintained by the University. The University's Covered Component receiving the request for amendment shall respond no later than sixty days after the receipt of the request. One thirty-day extension shall be permitted for the Covered Component to respond to the amendment request provided that the Covered Component provides the requesting individual with a written statement of the reasons for the delay and the date by which the Covered Component will complete its action on the request.

Requests for amendment of PHI shall be reported to the Office of Compliance Investigations, and Ethics.

The University's Covered Components shall develop procedures at the component level for making accepted amendments and inform the individual within the appropriate timeline. Support and forms are available upon request from the Office of Compliance, Investigations, and Ethics at compliance@pitt.edu.

If a University's Covered Component denies a request for amendment to PHI, the request for amendment and denial shall be forwarded to the Office of University Counsel and the Office of Compliance, Investigations, and Ethics for handling or disposition.

IV. Contact Information/Public Accessibility

This Procedure is posted under Administration & Operations Policies on the Office of Policy Development and Management's website and can be found at: https://www.policy.pitt.edu .

For specific questions related to this Procedure or HIPAA compliance at the University of Pittsburgh, please contact the Office of Compliance, Investigations, and Ethics at: compliance@pitt.edu .

V. Related Authorities

Policy AO [insert#], HIPAA

To comment on this draft Procedure, please click here.