WASHINGTON UNIVERSITY
Breach Notification – 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 define and appropriately address breaches of unsecured Protected Health Information ("PHI") in compliance with the HIPAA Breach Notification Rules and other applicable laws.

Scope of Policy

The scope of this Policy covers all Workforce members within Washington University covered entity component parts who become aware of a breach or suspected breach of PHI. Workforce members means employees (both faculty and staff), volunteers, trainees and other persons whose conduct, in the performance of work for Washington University, is under the direct control of Washington University whether or not they are paid by Washington University. The scope of this policy covers any breaches of PHI, the reporting requirements applicable to any such breach, and possible Sanctions.

Definitions

**Breach** means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security and privacy of the protected health information.

**Unsecured** PHI means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services. ePHI that has been encrypted according to the Washington University School of Medicine Encryption Policy is secured.

Policy

A Breach of PHI exists if there is an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rules and such action compromises the security or privacy of PHI (hereinafter “Breach”). Notification to the patient(s) or affected individual(s) must be made as soon as possible by the HIPAA Privacy Office, but in no case later than 60 days after discovery of Breach.

In order to assure that Washington University complies with its reporting obligations, all Workforce members must report any Breach or suspected Breach of PHI either directly to the HIPAA Privacy Office or to their supervisor or their Department’s HIPAA Liaison (if applicable), as soon as possible, but at least within 3 business days after discovery of the Breach or suspected Breach. If the Workforce member reports the Breach or suspected Breach to his or her supervisor or HIPAA Liaison rather than directly to the HIPAA Privacy Office, then it is that supervisor’s or Department Liaison’s responsibility to report the Breach or suspected Breach to the HIPAA Privacy Office as soon as possible. Failure of any Workforce member to comply with this policy will subject that Workforce member to Sanctions, as set forth in the Washington University HIPAA policy: “Sanctions for Non-Compliance with HIPAA Policies.”

Once notification of a Breach or suspected Breach is communicated to the HIPAA Privacy Office, that Office will undertake an investigation to assess whether, in fact, a Breach has occurred that mandates
reporting of the Breach to the affected individual(s), the U.S. Department of Health and Human Services (“HHS”), the media, or others. The HIPAA Privacy office will document the findings of its investigation and take the necessary steps to address any Breach as defined by the HIPAA regulations or other applicable laws.

Reporting Discovered Breaches

Upon discovering a Breach of PHI, the HIPAA Privacy office will take the following steps:

- For a single Breach involving 500 or more patients:
  - The affected individuals will be notified of the Breach by the HIPAA Privacy Office without unreasonable delay, but in no event more than 60 days following discovery of the Breach.
  - The HIPAA Privacy Office will notify HHS immediately;
  - Media in the jurisdiction in which the affected individual(s) resides will be alerted by the HIPAA Privacy Office in conjunction with Medical Public Affairs.
  - Substitute notice will be posted on the Washington University School of Medicine website and the HIPAA Privacy and Information Security websites.

- For a single Breach involving fewer than 500 patients:
  - The Affected individual(s) will be notified of the Breach by the HIPAA Privacy Office without unreasonable delay, but in no event more than 60 days following discovery of the Breach.
  - An electronic log detailing any such Breach will be maintained by the HIPAA Privacy Office and submitted to HHS annually.

Breaches of PHI discovered by Business Associate:

Under the same federal requirements, Business Associates must communicate any Breach of PHI to Washington University. Washington University HIPAA Privacy Office will prepare notification to affected individual(s) as necessary in accordance with this policy.

Access of PHI by WU Workforce Members

If a Washington University Workforce member inappropriately accesses a patient’s PHI for purposes other than for scheduling, patient care, billing, or other authorized purposes, the Workforce member will be subject to Sanctions as set forth in the Washington University HIPAA policy: “Sanctions for Non-Compliance with HIPAA Policies.” Additionally, the unauthorized access will be investigated by the HIPAA Privacy Office to determine whether this unauthorized access was a Breach under the Breach Notification Rules. If the access is determined to be a Breach, this policy will apply and all procedures herein will be followed, including notification to the affected individual of the Breach and the circumstances surrounding the Breach.

Violations of this Policy

Workforce members who violate this policy will be subject to Sanctions as set forth in the Washington University HIPAA Policy: “Sanctions for Non-Compliance with HIPAA Policies.” Additionally, if a University Department or any of its respective workforce members fail to secure electronic protected health information in accordance with the University Encryption Policy, the Department will be financially responsible for all costs and expenses associated with the Breach.

Last Revision Date: 4-4-13