HOWARD UNIVERSITY POLICY

Policy Number:	Clinical 900-001
Policy Title:	*HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996* BREACH NOTIFICATION POLICY
Responsible Officer:	Provost and Chief Academic Officer
Responsible Office:	Office of the Provost and Chief Academic Officer
Effective Date:	September 12, 2014

I. POLICY STATEMENT

The *Health Insurance Portability and Accountability Act of 1996* (HIPAA) establishes provisions for protecting the privacy and security of patient Protected Health Information (PHI). HIPAA requires that covered entities have and apply appropriate sanctions for workforce members who fail to comply with the privacy and security policies of the covered entity or the requirements of the Act. HIPAA regulations require covered entities and their business associates to provide notification following a breach of unsecured PHI. As a covered entity, Howard University ("the University") will make appropriate disclosures following a breach of unsecured PHI.

II. RATIONALE

This policy is required to provide for consistent identification and investigation of HIPAA privacy and security breaches in compliance with applicable law and regulation.

III. ENTITIES AFFECTED BY THIS POLICY

This policy applies to all entities within the University enterprise including, but not limited to, Sponsored Research, Office of Regulatory Research Compliance, Office of Research Development, Howard University Hospital (HUH), and all business associates.

IV. DEFINITIONS

A. **Business Associate -** A person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provides services to, a covered entity.

B. **Breach** - The acquisition, access, use or disclosure of (1) Protected Health Information in a manner which compromises the security or privacy of the Protected Health Information, or (2) other personal information within the meaning of

applicable state law in a manner which compromises the security or privacy of such information.

A breach excludes:

1. Any unintentional acquisition, access or use of Protected Health Information by a workforce member or person acting under the authority of Howard University or a business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure.

2. Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Howard University or a business associate to another person authorized to access Protected Health Information at Howard University or a business associate, or organized health care arrangement in which Howard University participates, and the information received as a result of such disclosure is not further used or disclosed.

3. A disclosure of Protected Health Information where a Howard University or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

C. **Privacy Officer –** The designated individual in the Office of the Chief Compliance Officer who is responsible for the development and implementation of HIPAA policies and procedures for the enterprise.

D. **Protected Health Information (PHI) –** Information transmitted or maintained in any form that is created or received by a health care provider, health plan, health care clearinghouse, or employer and: (1) relates to the past, present, or future physical or mental health or condition of a patient, the provision of health care to a patient, or the past, present, or future payment for the provision of health care to a patient; and (2) identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient. It does not include certain education records and health information of students covered by the Family Educational Rights and Privacy Act. It does not include employment records held by a covered entity in its capacity as employer. It does not include individually identifiable health information regarding a person who has been deceased for more than 50 years.

E. **State Law** –The state or District of Columbia laws requiring disclosures of breaches of personal information of persons located in those jurisdictions.

F. **Unsecured Protected Health Information -** Protected Health Information that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or other methodology specified by the U.S. Department of Health and Human Services Secretary in the guidance issued under section 13402(h)(2) of the Public Law 111-5.

G. **Workforce Members –** Faculty, staff, employees, volunteers, contractors, students, trainees, and other persons whose conduct, in the performance of work for Howard University, is under the direct control of Howard University, whether or not they are paid by Howard University.

V. POLICY PROCEDURES

A. Identifying a Breach

An impermissible use or disclosure of PHI is presumed to be a breach unless Howard University or the business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the Protected Health Information or to whom the disclosure was made;

3. Whether the Protected Health Information was actually acquired or viewed; and

4. The extent to which the risk to the Protected Health Information has been mitigated.

B. Breach Notification

The Privacy Officer, following the discovery of a breach of unsecured PHI, shall notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of such breach.

1. Notification shall be without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, subject to any law enforcement delay.

2. Written notification shall be sent by first-class mail to the individual at his/her last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings, as information is available.

3. If the individual is deceased and the address of the next of kin or personal representative is known, written notification by first class mail shall be sent to either the next of kin or personal representative. The notification may be provided in one or more mailings, as information is available.

4. Written notification shall be written in plain language and shall include, to the extent possible:

(a) A brief description of what happened.

(b) The date of the breach.

(c) The date of the discovery of the breach, if known.

(d) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

(e) Any steps individuals should take to protect themselves from potential harm resulting from the breach.

(f) A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

(g) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address.

For a breach of unsecured PHI involving *more than* 500 individuals:

The Privacy Officer shall, following the discovery of the breach and after consultation with the Chief Compliance Officer and upon approval by the General Counsel, notify the U.S. Health and Human Services (HHS) Secretary, using the official HHS reporting form, of the breach of PHI immediately (without unreasonable delay and in no case later than 60 calendar days after discovery of a breach).

The instructions on the HHS website and applicable regulations shall be followed when submitting the above information.

The Privacy Officer shall, after consultation with the Chief Compliance Officer and upon approval by the General Counsel, work with the Office of University Communications to ensure that the appropriate notification to the media of a breach of PHI is made no later than 60 days after the discovery of the breach of PHI. This notification shall also be coordinated with any notifications required under other local, state or U.S. laws.

For a breach of unsecured PHI involving *fewer than* 500 individuals:

The Privacy Officer shall maintain a log of breaches of PHI and complete HHS's online form or other applicable procedures for each individual breach no later than 60 days after the end of each calendar year.

Instructions on the HHS website shall be followed when submitting the above information.

C. **Notification by a Business Associate**

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the Privacy Officer following the discovery of the breach.

A business associate must report any unauthorized use or disclosure of Protected Health Information, including breaches of unsecured PHI as required at 45 C.F.R. § 164.410, within three (3) days. The notice shall include: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach; (2) the identification of each individual whose unsecured PHI was breached; (3) a description of the types of unsecured PHI that were involved in the breach; (4) any steps individuals should take to protect themselves from potential harm resulting from the breach; and (5) a brief description of what the business associate is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches.

D. **Workforce Training**

The Office of the Chief Compliance Officer will offer training on HIPAA policies and procedures as necessary and appropriate for the members of the work force to carry out their functions and to facilitate institutional compliance. HIPAA training is a component of the Compliance Training and Education Program.

E. **Duty to Report**

Howard University workforce members and business associates shall notify the Privacy Officer immediately if the workforce member or business associate becomes aware of any information concerning a possible unauthorized disclosure of Protected Health Information.

F. **Breach Investigation**

The Office of the Chief Compliance Officer will be responsible for conducting the investigation into the circumstances, scope and required remedial measures (including notifications) associated with a breach and will draw on resources in other areas as appropriate. For breaches involving more than 500 individuals, a business associate or another covered entity, the Office of the Chief Compliance Officer will work with and pursuant to the direction of the Office of General Counsel. In such circumstances, the investigation shall be regarded as privileged, and no information gathered in the course of the investigation may be disclosed to others without authorization of the Office of General Counsel, except as may be needed to comply with any notification or other regulatory requirements.

No person shall be involved in the investigation if she or he was directly involved in the circumstances leading to the breach (such person a "Conflicted Person"), absent express permission from the Office of General Counsel. If, during the course of an investigation, it becomes apparent that a person involved in the investigation may have a conflict of interests ("Conflicted Person"), she or he must recuse her- or himself immediately and notify the Office of General Counsel of the basis for such recusal.

G. **Logging and Document Retention**

The Office of the Chief Compliance Officer will maintain a breach notification log containing all reported potential unauthorized disclosures, the date of the report, as well as the date and a summary of the breach notification assessment. The log will also track the date of all notifications to patients, the U.S. Department of Health and Human Services and the local media. All information concerning HIPAA breach notifications will be maintained for a minimum of six years as required by the HIPAA breach notification rule.

H. **State Laws**

State laws (including the laws of the District of Columbia, Maryland and Virginia) impose certain requirements in the event of breach of personal information of persons located in those jurisdictions. Whether an incident is a breach that requires reporting, and the associated requirements and timelines for those reports, will be assessed on a case-by-case basis for each state.

VI. SANCTIONS

Failure to follow this policy or any other approved University policy shall be subject to disciplinary action, up to and including termination of employment.

VII. HYPERLINKS

www.howard.edu/policy

Related Policies and Regulations:

- *Health Insurance Portability and Accountability Act of 1996* (45 Code of Federal Regulations Part 160, Part 162 and Part 164)

- US Department of Health and Human Services (HHS), hhs.gov, Health Information Privacy, HHS Breach Notification Report Forms, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html