HOWARD UNIVERSITY POLICY

Policy Number:	Clinical 900-002
Policy Title:	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY AND SECURITY VIOLATIONS/SANCTIONS POLICY
Responsible Officer:	Provost and Chief Academic Officer
Responsible Office:	Office of the Provost and Chief Academic Officer
Effective Date:	February 3, 2015

I. POLICY STATEMENT

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Act") 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. Howard University ("University") workforce members may access, use and disclose PHI only as permitted by law and as authorized by the University to perform their job responsibilities. Access, use and/or disclosure outside the scope of the job without authorization, or to assist others to improperly access, use or disclose PHI, is strictly prohibited. It is University policy to take disciplinary action against workforce members who violate HIPAA or the University's privacy and security policies.

II. RATIONALE

This policy is required to provide for consistent and appropriate sanctions against workforce members who fail to comply with the privacy and security policies and procedures of Howard University and/or HIPAA.

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 the Faculty Practice Plan.

IV. DEFINITIONS

A. **Breach** - The acquisition, access, use or disclosure of (1) PHI in a manner which compromises the security or privacy of the PHI, or (2) other personal information within the meaning of applicable District of Columbia or other 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 PHI 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 PHI at Howard University or a business associate to another person authorized to access PHI 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 PHI where a Howard University workforce member 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.

B. Business Associate - A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, the University.

C. Health Care Operations - Includes administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities include, but are not limited to: business management and general administrative activities, quality assessment and improvement, training health care and non-health care professionals, accreditation, certification, licensing, credentialing, medical review, legal and auditing services, customer service, and resolution of internal grievances.

D. Payment - The activities undertaken by a health care provider to obtain reimbursement for the provision of health care and the activities related to the individual to whom health care is provided, including but not limited to: (i) determinations of eligibility for coverage and adjudication or subrogation of health benefit claims; (ii) adjusting risk amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance and related health care data processing; (iv) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: (a) name and address, (b) date of birth, (c) social security number, (d) payment history, (e) account number, and (f) name and address of the health care provider or health plan.

E. **Privacy Officer** – The designated individual in the Office of the Chief Compliance Officer for Health Sciences (hereafter "Office of the Chief Compliance Officer") who is responsible for the development and implementation of HIPAA privacy policies and procedures for the enterprise.

F. **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.

G. **Security Officer** - The designated individual in the University's Office of the Chief Information Officer who is responsible for the development and implementation of HIPAA security policies and procedures for the enterprise.

H. **Treatment** – Includes the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

I. **Unsecured PHI -** PHI 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.

J. **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. Permitted Use or Disclosure

Workforce members are permitted to use or disclose PHI, within the scope of the individual workforce member's job responsibilities, in the following instances:

1. To the individual who is the subject of the PHI.
2. In compliance with consent to carry out treatment, payment or health care operations.

3. Without consent, if consent is not required and has not been sought.
4. In compliance with valid authorization.
5. Pursuant to an appropriate Business Associate Agreement.

B. Non-Permitted Use or Disclosure of PHI

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 PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

C. Violations

Howard University's Privacy Officer will investigate all alleged HIPAA privacy violations. All alleged HIPAA security violations will be investigated in tandem by the Privacy Officer and Security Officer.

Violations of the University's HIPAA privacy and security policies will lead to disciplinary action in accordance with applicable University policies and procedures, regardless of whether the violation leads to a privacy or security breach. Any such violations of HIPAA policies may also be taken into account in such individual's performance evaluation. The Office of the Chief Compliance Officer is charged with enforcement of all HIPAA policies and shall work with the impacted departments and the Office of Human Resources to identify appropriate disciplinary measures.

The categories of offenses listed below, while not all inclusive, are organized according to the severity of the violation.

LEVEL 1 - Accidental or inadvertent violation: This is an unintentional violation of privacy or security policies that may be caused by inattentiveness, lack of understanding, lack of training, or other human error.

Examples include but are not limited to:

- Directing PHI via mail, e-mail or fax to the wrong party.
- Incorrectly typing a patient's medical record number and viewing the incorrect patient's PHI.

LEVEL 2 - Failure to follow established privacy and security policies and procedures: This level of offense typically is indicative of unsatisfactory job performance or lack of performance improvement.

Examples include but are not limited to:

- Release of PHI without proper patient authorization.
- Leaving detailed PHI on an answering machine.
- Failure to report privacy and security violations.
- Improper disposal of PHI.
- Failure to properly sign off from or lock computer when leaving a work station.
- Failure to properly safeguard password or username.
- Sharing passwords or usernames with others.
- Using another workforce member's password or username.
- Failure to safeguard portable devices from loss or theft.
- Transmission of PHI using an unsecured method.
- Discussing confidential information in a public area.
- Repeat of Level 1 Violation.

LEVEL 3 - Unauthorized use and/or misuse of PHI or records: This level of breach occurs when a workforce member intentionally accesses or discloses PHI in a manner that is inconsistent with policies and procedures, but for reasons unrelated to personal gain.

Examples include but are not limited to:

- Accessing information that one does not need to know to do his or her job.
- Looking up a co-worker's address from medical records to send a sympathy card.
- Informing an individual that you saw a family member at Howard University's health care facilities.
- Reviewing a public official or celebrity's PHI.
- Reviewing the medical record of a co-worker, family member or acquaintance.
- Circumventing established procedures for handling of PHI in order to perform a designated task more quickly or efficiently.
- Storing PHI on an unencrypted device.
- Failing to cooperate with an investigation by the Chief Compliance Officer, Privacy and/or Security Officer.
- Repeat of Level 2 Violation.

LEVEL 4 – Willful and/or intentional disclosure of PHI or records: This level of violation occurs when a workforce member accesses, reviews or discloses PHI for personal gain or with malicious intent.

Examples include, but are not limited to:

- Reviewing a record to use information in a personal relationship.
- Compiling a mailing list for personal use or to be sold.
- Posting PHI to social media Web sites.
- Disclosing a celebrity or public official's PHI to the media for personal gain.
- Repeat of Level 3 Violation.

VI. SANCTIONS

Workforce members found to have violated HIPAA will be disciplined, up to and including termination. Sanctions may include but are not limited to HIPAA counseling, retraining, written reprimand, unpaid suspension or termination.

A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA may face criminal and civil penalties under federal and state law.

Except where otherwise required by law, the type of sanction administered by the University will depend on the intent of the individual and severity of the violation. The Office of the Chief Compliance Officer will work with the impacted departments, the Office of Human Resources and General Counsel, where necessary, to determine intent and severity of the violation.

VII. HYPERLINK

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)

- 900-001 *Health Insurance Portability and Accountability Act of 1996 Breach Notification Policy*