MONMOUTH UNIVERSITY
POLICIES AND PROCEDURES

Policy Name: **Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Policy**

Original Issue Date:	April 1, 2004	**Revision Date:**	February 18, 2011
Approved By:	President and Cabinet	**Issued By:**	Patricia Swannack Vice President for Administrative Services

I. Purpose

Monmouth University, pursuant to the Health Insurance Portability and Accountability Act (HIPAA) law and regulations, is required to take reasonable steps to ensure the privacy of your Protected Health Information (PHI). PHI is individually identifiable health information related to past, present or future physical or mental health or condition of an individual; provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. PHI includes, but is not limited to, information such as name, address, zip code, social security number, driver's license number, date of birth, medical record, etc. Employees are expected to adhere to the University's rules and regulations. Employees who disregard University policies and procedures and /or related State or Federal laws and regulations will be subject to disciplinary action up to and including termination.

II. Scope of Policy

A. The primary mission of Monmouth University is education and only part of our activities include covered functions under the HIPAA Privacy Rule. Monmouth University has determined that it is a hybrid entity for the purposes of HIPAA and the following has been determined to be a covered component: Monmouth University Healthcare Flexible Spending Account Plan.

B. The following are also designated as part of the hybrid covered entity to the extent that they perform activities associated with the above component related to administrative functions of the plan:

1. Office of Human Resources
2. Office of Payroll
3. Office of the Controller
4. Office of Internal Audit
5. Information Management
6. Office of the General Counsel

III. Privacy Official

The University has appointed a Privacy Official, (Director of Benefits and Training) to ensure compliance with HIPAA laws and regulations for all healthcare components included in this Privacy Policy. The Privacy Official is responsible for the development, implementation and update of policies, procedures and training programs that will insure compliance with HIPAA Privacy and will respond to all requests related to individual PHI. The Privacy Official will consult with and rely on advice of counsel from the Office of the General Counsel.

IV. Notice of Privacy Rights

A. Pursuant to applicable law and regulations, you have the following rights regarding your PHI:

1. The right to receive a copy of the "Notice of Privacy Practices."
2. The right to request restrictions on disclosures for treatment, payment of benefits and/or health care operations.
3. The right of access to inspect your own PHI.
4. The right to an accounting of all uses and disclosures of your PHI in the previous 6 years, except for treatment, payment or healthcare operations.
5. The right to amend your PHI (created by any healthcare component).
6. Right to confidential communications about PHI.
7. The right to file a complaint if you believe your rights have been violated.

B. The Notice of Privacy Practices will be individually delivered to all participants of any healthcare component listed in Section II.A above immediately upon enrollment in such plan, within sixty (60) days after a material change to the notice, and at least once every three years.

V. Safeguarding of PHI

A. The University will limit the use and disclosure of PHI to only the Covered Entity, a Business Associate if applicable, or as permitted or required by law. Such disclosure will be for the purpose of payment of benefits, claim resolution, enrollment/disenrollment and healthcare component operations and pursuant to legal process.

B. Information deemed to be PHI will be secured in authorized offices only (i.e., Office of Human Resources, Office of the Controller, and the Office of Payroll) and will be accessible to only those individuals who need access to or may come in contact with PHI, who have been trained in HIPAA compliance and who have signed confidentially agreements with Monmouth University.

C. All PHI will be kept in secured file cabinets in offices that are locked overnight. If any employee who is not authorized has access to the office(s) during non working hours, then the PHI must be kept in locked file cabinets and/or safe, with access limited to authorized personnel only.

D. PHI pertaining to the University's healthcare components includes but is not limited to employee enrollment and disenrollment information, employee contribution amounts and reimbursement payments from the plan to individual participants. Human Resources may receive claim information from an employee, with the appropriate signed authorization form from the employee, in cases of resolving claim issues. The information will remain confidential and will be kept in a secured file cabinet housed in the Office of Human Resources.

VI. Training

A. The Privacy Official will schedule HIPAA compliance training for all current employees and any new employees who may assume such responsibilities and are authorized to have access to, or may come in contact with PHI.

B. Additional training will be provided for authorized employees when and if any changes are made to the Privacy Rules within a reasonable period of time after the material change becomes effective.

C. All authorized employees who may have access to, or may come in contact with PHI will be required to sign a University HIPAA Confidentiality Agreement.

VII. Complaints

A. The Privacy Official will be the University's contact person for receiving complaints.

B. If an employee believes his/her rights have been violated, he/she may file a complaint utilizing the University's HIPAA Complaint Procedure.

C. An employee may complain in writing to the Privacy Official in Human Resources. (See attached HIPAA Complaint Form).

D. Complaints may also be made in writing to the Secretary of the U.S. Department of Health and Human Services. (See attached HIPAA Complaint Procedures).

E. Complaints must be made within 180 days after the employee knows or should have known about the act or omission that is the subject of his/her complaint.

F. Any healthcare component and the employer may not intimidate, threaten, coerce, discriminate against or take any retaliation against any employee who exercises any right under the Privacy Rule; files a

complaint with the Secretary of HHS; testifies, assists or participates in an investigation or other proceeding under the Privacy Rule; or opposes any unlawful practice under the Privacy Rule in good faith.

VIII. Sanctions

Any employee who fails to comply with HIPAA laws and regulations as detailed in the University HIPAA Privacy Policy and Procedure will be subject to disciplinary action up to and including termination.

IX. Record Retention

The University will maintain the policies and procedures, all communication, documentation of any action, activity or designation that are required by the Privacy Rule to be in writing, in written or electronic form, for at least six years from the date of its creation or the date when it last was in effect, whichever was later.