

**OFFICE OF ADMINISTRATION & FINANCE
ADMINISTRATIVE MEMORANDUM**



DATE: March 10, 2006

NUMBER: HR-03

TITLE: Confidentiality and Privacy

PURPOSE

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress and signed into law in 1996. Originally, the focus of HIPAA was confined to certain health insurance-related issues. HIPAA now also focuses on Title II, Subtitle F, the section that deals with Administrative Simplification and Privacy.

The following policy and procedures have been established to assure the privacy, security, and confidentiality of protected health information (PHI) consistent with the Pennsylvania State System of Higher Education Privacy and Security Policy for Health Plans and *Management Directive 505.18, Maintenance, Access and Release of Employee Information*.

In addition, with the implementation of the Shared Administrative System Human Resource/Payroll module using SAP technology, it is essential that the confidentiality and privacy of this information also be maintained.

SCOPE

This policy applies to all University employees in any action undertaken in the name of, for the benefit of, or as part of their activities relative to the University.

POLICY

This policy is designed to protect the legal rights of all employees against breach of confidentiality. Such information includes personnel and/or health information and other confidential statements and/or materials. Specifically, this may include:

- Protected health information (PHI)
- Access to personnel files
- Access to Human Resources/Payroll module of SAP
- Personnel transactions, including but not limited to, employment information, performance evaluations, disciplinary actions, leave information, and grievances
- Insurance and litigation information

Additionally, this policy establishes privacy protections that ensure the interests of employees and limit exposure to allegations of breach of privacy and breach of the employees' duty of confidentiality.

Unauthorized accessing of any record (whether electronic or manual), divulging confidential information to an unauthorized third party, using confidential information for personal use, and/or

inappropriately removing confidential information from University property are strictly prohibited and may result in disciplinary action, up to and including termination of employment.

PROCEDURES

1. PHI will be maintained and confidentially stored in the Office of Human Resource Management until such time as the healthcare issue, claim, etc. has been resolved. Once resolved, the PHI will be destroyed and no copies kept.
2. This information will be kept locked and separate from all other records and accessible only as permissible by this policy. Records will not include any PHI on a label or any other portion of the outside folder.
3. Documentation of all disclosures of PHI, including disclosures to the employee or pursuant to an authorization, will be maintained for a minimum of six years. That documentation will include the date of the disclosure; the name of the person or entity who received the PHI and, if known, the address; a brief description of the PHI disclosed; and a brief statement as to the purpose of the disclosure.
4. The University Benefits Manager will only use or disclose PHI to the individual employee; pursuant to, and in compliance with, an authorization that complies with HIPAA Privacy and Security procedures; pursuant to an agreement by the employee to use or disclose to a family member, other relative, or close personal friend of the employee to such extent as may be relevant; or as otherwise permitted by and in compliance with the HIPAA Privacy Regulations or by law.
5. All employees who have been given access in SAP will be required to sign a *Confidentially Statement* (Attachment A) assuring that they will access, use, discuss, release, and/or divulge only the data that is needed to perform their job.
6. Use of and collection of Social Security numbers (SSNs) will be restricted to circumstances necessary for proper administration of lawful business. Access to SSNs will be limited to those with a legitimate need in the performance of their duties. Employees should use their payroll identification numbers on most forms formerly requiring the use of SSNs. Documentation containing SSNs must be placed in a sealed envelope in which the SSN is not visible. SSNs sent through electronic media should be done only when necessary and with encryption or a secure connection.
7. Any signed *Confidentiality Statement* will be maintained in the individuals' official personnel record.
8. Personnel files are the property of the University and access to the information they contain is restricted. Generally, only management officials and representatives of the University who have a legitimate, verifiable reason to review information in a file are allowed to do so.
9. With advance notice of one business day, an employee may review material in his or her file but only in the presence of a representative of the Department of Human Resources or a representative of the Provost's Office in the case of a faculty member. Such examination must be done within normal business hours. The employee may be charged a reasonable fee for copying any requested materials.

10. Information in a personnel file will not be disclosed to anyone outside the University without a signed consent from the employee specifically authorizing the release of the information, except as listed below:
 - a) Basic information such as employment, work telephone number, and job title may be verified without notification to the employee.
 - b) The Department of Human Resources will comply with lawfully issued subpoenas and judicial orders.
11. In most cases, the University will use a progressive disciplinary system addressed through documentation and counseling for any violations of this policy. Some violations, however, are more serious in nature and may result in immediate termination of employment.
12. Whenever there is a change in law that necessitates a change to these policies and procedures, the Office of Human Resource Management will promptly document and implement the revised policy and procedure.

ROLES AND RESPONSIBILITIES

1. The University Benefits Manager is responsible for receiving and processing requests for access to PHI.
2. The Office of Human Resource Management will exercise due diligence in the maintenance, use, storage, and sharing of employee information. Files containing SSN information will be locked. Documentation containing SSNs that is subject to disposal will be shredded prior to disposal.
3. The Office of Human Resource Management will maintain an environment to support the privacy and security of employee information.
4. The Office of Human Resource Management will provide training to employees on this policy and will recommend the appropriate sanctions for non-compliance.
5. The Office Human Resource Management will maintain and submit records as may be necessary to comply with federal and state laws and regulations.
6. All Human Resource Management employees will abide by state and federal laws and regulations and the procedures set forth in this policy. Except under limited circumstances, no PHI, written or oral, can be disclosed without written consent of the employee.
7. All University employees are responsible for not keeping PHI in their e-mail account, or an unlocked computer screen, or maintained in a non-secure area.

This policy will become effective immediately.

**Pennsylvania State System of Higher Education
Confidentiality Statement**

Background

With the implementation of the Shared Administrative System Human Resource/Payroll module using SAP technology, more information will be stored in an electronic format. It is essential that the confidentiality and privacy of this information be maintained. As a Pennsylvania State System of Higher Education (System) employee who has been given access to confidential information, it is your responsibility to protect this sensitive and personal data.

System management and employees are relying on you to maintain confidentiality of the employee data and to access, use, discuss, release, and disclose this data only when it is dictated by your job duties. If you do not need to access employee information to perform your job, under no circumstances should it be accessed. If you do need to access employee information to perform your job, the information should not be divulged to anyone unless it is done so through authorized protocols.

To ensure that all System employees with access to SAP Human Resource/Payroll System information are aware of this confidentiality requirement, you must sign and date the statement below. You should retain a copy of this notice for your records and return the original copy of this form to the human resource office. If you have any questions regarding your responsibility to maintain confidentiality of the data to which you have access in your work associated with the SAP Human Resource/Payroll system, you should contact the Director of Human Resource Management.

CONFIDENTIALITY STATEMENT

As an employee of the Pennsylvania State System of Higher Education (System), I understand that I may have access to confidential, personal data of System employees. I agree that I will access, use, discuss, release, and/or divulge only the data that is needed to perform my job. I understand that I am prohibited from accessing, using, discussing, releasing, and/or divulging this data unless doing so is a requirement of my job. I understand that any release of this information will be done only through authorized protocols. For System employees, breaches in confidentiality of such data may result in disciplinary action up to and including separation from employment. A violation of this agreement also may result in criminal action if it is determined that any local, state, or federal law has been violated.

By my signature below, I am certifying that I have read, understand, and agree to abide by the provisions of this policy.

Signature

Date

Print Name

University