Date Published: 9-28-2016

Customer and Personally Identifiable Information - Security Policy - Interim

UNIVERSITY OF HEALTH SCIENCES & PHARMACY in St. Louis

College Services & Information Technology
Customer and Personally Identifiable Information - Security Policy - Interim

Applies to: (examples; Faculty,Staff, Students, etc)

Faculty , Staff , Students , Contractors_Vendors

Policy Overview:

Issued: 09-28-2016

Next Review Date: 06-15-2022

Frequency of Review: Annually

University of Health Sciences and Pharmacy in St. Louis (the "University") has developed this policy to ensure that appropriate guidelines are followed to protect the privacy of Customer Information ("CI") and Personally Identifiable Information ("PII") maintained or used by the University.

Applies to all faculty, staff, student workers, and temporary employees or third-parties with access to CI or PII.

Definitions:

Customer Information ("CI") means any record containing nonpublic, personally identifiable financial information about a student or Customer of the University, whether in paper, electronic, or other form that is handled or maintained by or on behalf of the University or its affiliates. For purposes of this Policy, the term shall cover any information (i) an employee, student or third party provides in order to obtain a financial service from the University, (ii) about an employee, student or third party resulting from any transaction with the University involving a financial service, or (iii) otherwise obtained about an employee, student or third party in connection with offering or providing a financial service to that person. Examples of a covered financial product or service include offering or providing credit or debit cards and student loans, grants, or scholarships. Examples of CI includes information received in connection with a financial product or service such as tax or financial information from a student or the student's parent in connection with a financial aid award or application, income and credit histories relating to a credit card or loan application, and information about a financial services transaction such as the current account balance, amount of funds transferred or disbursed to a student, or debt collection activity. Generally, nonfinancial information about students or employee benefits related information such as retirement plan participation levels are subject to confidentiality or security requirements under FERPA, ERISA, or other applicable laws.

Information Security Program ("ISP") means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle CI and PII.

ISP Coordinator means, with respect to electronically stored or transmitted information, the University's Chief Information Officer, and, with respect to physically stored information, the Vice President, Operations and Chief Compliance Officer. The ISP Coordinator shall be responsible for coordinating and overseeing the ISP including, without limitation, compliance with the required components of the ISP and maintaining satisfactory documentation of ISP activities for audit and reporting purposes.

Personally Identifiable Information ("PII") means information or data that is stored or transmitted in paper, electronic, or other form that involves an individual's first name or first initial and last name in combination with any one of the following data elements that relate to the individual if the data elements are not encrypted, redacted, or otherwise altered by any method or technology that renders the information unreadable or unusable: social security number, driver's license or unique identification number created or collected by a government body, financial account number, credit or debit card number in combination with any required security code, access code, or password, medical information, or health insurance information. PII also includes information that consists of direct or indirect identifiers covered under the Family and Educational Rights to Privacy Act including the name and address of the student or family member, unique identifiers, date or place of birth, parent's names, or other information which can be used to determine the identity of the student directly or indirectly through linkages to other information.

Details:

The University has implemented this policy to comply with federal and state laws and meet the privacy expectations of its faculty, staff, students, vendors, and the general public. This policy outlines the components of the University's ISP to protect CI and PII received, maintained, or used by the University. The critical components of the ISP include: 1) designation of a ISP Coordinator responsible for regularly identifying and assessing risk on an established schedule and after a suspected or actual breach or incident, 2) designing and implementing safeguards to control risks identified through risk assessment, (3) regularly testing or monitoring the effectiveness of the safeguards' key controls, systems, and procedures, 4) overseeing the selection of third party service providers and protecting covered information through appropriate contracting practices, and 5) evaluating and making adjustments to the ISP as a result of testing or monitoring, material changes to operations or business arrangements, or circumstances that may have a material impact on the ISP. This policy supplements existing University and departmental policies applicable to the privacy and security of records.

CI and PII Security Guidelines

1. Collection and access to CI or PII must be requested by an individual's supervisor or area administrator. Supervisors and administrators are responsible for maintaining their area's secure work processes with CI or PII and requesting removal of access to CI or PII when an individual's employment or responsibilities change.
2. All employees must comply with the University's policies governing confidentiality and disclosure of personally identifiable information contained in education records covered by FERPA.
3. All employees must comply with the University's policies governing access and security of IT equipment, devices, and systems.
4. Employees are to refrain from asking students for their social security number unless required by the tasks and responsibilities associated with their job.
5. Collecting, accessing and disseminating CI or PII is strictly prohibited unless required by tasks and responsibilities associated with an employee's job.
6. Electronic transmission by e-mail and/or other social media of CI or PI is prohibited unless software and/or method of transmission has been approved by the IT Department.
7. It is prohibited to leave CI or PII unattended in a non-secure environment.
8. It is prohibited to store CI or PII in a non-secure environment such as an unlocked cabinet.
9. Employees who have permission to work with CI or PII are not permitted to download files containing such information to portable media (e.g., flash drives, PDA's), laptops and/or University Office PC hard drives. This also includes non-University digital storage solutions, such as Dropbox and personal cloud services.
10. Employees are prohibited from discarding paper documents containing CI or PII that are not "cross-shredded" into trashcans or unsecured paper recycling containers.
11. Employees are required to seek permission from and adhere to the University Operations Department's instructions and procedures pertaining to the archiving and/or destruction of paper documents containing CI or PII.
12. Employees are required to notify their immediate supervisor of any actual or suspected breach of security involving CI or PII. Supervisors are then required to notify a member of the University's Incident Response Team as provided in the Incident Response Plan Policy. For example, a breach may involve a lost or stolen computer or other device containing unencrypted CI or PII or the unauthorized access of such information. If employees are uncertain whether there has been a breach, they must be advised to report the event to their supervisor.
13. All contracts entered with third-party providers are required to contain appropriate acknowledgement of security measures for CI or PII by the third party. (See form attached).
14. Departments will designate a person and procedure for referring calls or other requests for CI or PII to designated individuals within the department, the Registrar, Business Office, human resources, or other responsible unit.
15. Employees will not share passwords with others or post them in an unsecure location.
16. When faxing CI or PII, the sender should ensure that the recipient is available to receive the fax and validate the number of pages received or that the receiving fax requires a PIN or other form of identification to receive the information.
17. Adequate security measures such as encryption will be implemented when storing or transmitting CI or PII in electronic form.
18. A chain of custody form or Confidentiality label should be used when transmitting, forwarding, or storing CI or PII.
19. Individuals having access to CI or PII will be required to sign a Confidentiality Agreement.
20. Upon termination of employment or a contract, employees or persons with access to CI or PII will return all CI or PII and their access will be revoked.

Policy Violations

1. Violations of any part of this policy resulting in the misuse, unauthorized access, or unauthorized disclosure or distribution of CI or PII will be subject to University disciplinary procedures, up to and including the termination of employment or contract with the University. The University will contact law enforcement authorities whenever suspected criminal activity is involved.

Procedures:

I. **Risk Identification and Assessment.** The University will take steps to identify and assess external and internal risks to the security, confidentiality, and integrity of CI and PII that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the ISP, the ISP Coordinator will establish procedures for identifying and assessing such risks in each relevant area of the University's operations, including:

a. Employee training and management. The ISP Coordinator will coordinate with the Director of Human Resources and the President's Staff to disseminate this policy and evaluate the effectiveness of the University's procedures and practices relating to training for employees whose duties involve access to and use of CI and PII.

b. Information Systems and Information Processing and Disposal. The ISP Coordinator will coordinate with representatives of the University's Department of Information Technology or other relevant department to assess the risks to CI and PII associated with the University's information systems, including network and software design, information processing, and the storage, transmission and disposal of CI and PII. This evaluation will include assessing the University's current policies and procedures relating to acceptable use of the University's network and network security, document retention and destruction. The ISP Coordinator will also coordinate with the University’s Department of Information Technology to assess procedures for monitoring potential information security threats associated with software systems. Monitoring will be conducted reasonably to ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified. Monitoring may include sampling, system checks, reports of access to systems, review of logs, audits, and any other reasonable measures adequate to verify that the ISP’s controls, systems and procedures are working. All procedures and responses will be reviewed against best practices and standards published by the Federal NIST Computer Security Resource Center.

c. Detecting, Preventing and Responding to Attacks. The ISP Coordinator will coordinate with the University’s Department of Information Technology, Business Office, Enrollment Services, Financial Aid, Human Resources and other relevant units to evaluate procedures for and implement methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the ISP Coordinator has primary responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the University. Security systems will include maintaining and implementing current anti-virus software, installing patches to correct software vulnerabilities, maintaining appropriate filtering or firewall technologies, alerting the University community of security threats, imaging documents and shredding paper copies, backing up data regularly and storing back up information off site, and other reasonable measures to protect the integrity and safety of information systems.

II. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of CI and PII, whether in electronic, paper or other form. The ISP Coordinator will, on a regular basis, implement administrative, technical and physical safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing monitoring, detection, and problem escalation procedures. The ISP Coordinator will take the following steps to protect the security and integrity of CI and PII:

a. Maintain a registry of all computers attached to the University’s network including, relevant IP address or subnet, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person(s) and unit with primary responsibility for the device, and whether the device contains or has access to any CI and PII.
b. Assure that security patches for operating systems or software environments are current or updated as needed.
c. Maintain a data handbook listing those persons and offices responsible for CI or PII and the type of covered data in physical storage or software systems.
d. Maintain a current registry of persons with access to covered data and information.
e. Assure the physical security of all file cabinets, storage areas, servers and terminals which contain or have access to covered data and information by using secure access methods including, without limitation, locking mechanisms, password-protection, encryption, secure connections for transmitting data outside the University, using secure servers, prohibiting storage of covered data on transportable media (USB, flash drives etc.) and non-University digital storage solutions, permanently erasing covered data from computers , magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposing of them, storing physical records in a secure area protected from physical hazards such as fire or water damage, disposal of outdated records pursuant to the University’s Record Retention Policy, and other reasonable measures to secure covered data during its life cycle in the University’s possession or control.
f. Use encryption to protect all electronic covered information including data bases and information in transit.
g. Require user-specific passwords and periodic change of user-specific passwords, limiting access to covered information on a need for access basis, signed certification of responsibilities prior to authorizing access to systems with covered data, requiring signed releases for disclosure of covered data, and automatic lock out for multiple failed log-in attempts.
h. Establish methods for prompt reporting of loss or theft of covered data or media upon which data may be stored.
i. Implement network and software systems designed to limit access and maintain appropriate screening ISPs to detect computer hackers and viruses.

III. Overseeing Service Providers. The ISP Coordinator shall coordinate with those responsible for third party service procurement activities among the Department of Information Technology and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for CI and PII of students and other third parties to which they will have access. In addition, the ISP Coordinator will work with the Office of General Counsel to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the ISP Coordinator and Office of General Counsel. These standards shall apply to all existing and future contracts entered into with such third party service providers.

IV. Adjustments to ISP. The ISP Coordinator is responsible for evaluating and adjusting the ISP based on the risk identification and assessment activities undertaken pursuant to the ISP, as well as any material changes to the University’s operations or other circumstances that may have a material impact on the ISP. The ISP Coordinator will provide a report on the status of the ISP each year as part of the annual risk management assessment under the Enterprise Risk Management Policy.

Responsibilities:

Position/Office/Department	Responsibility
Assistant Vice President, IT	The Assistant Vice President for IT serves as the ISP Coordinator for electronically stored or transmitted CI and PII. The ISP Coordinator may designate

	other representatives of the University to oversee and coordinate particular elements of the ISP. Any questions regarding the implementation of the ISP or the interpretation of this document should be directed to the ISP Coordinator.
General Counsel	Provides general legal advice on compliance with applicable federal and state laws and regulations. Assists with third party contracts involving CI or PII to incorporate adequate protections into the contract.
Vice President, Operations & Chief Compliance Officer	Coordinates and oversees security and integrity of physical documents containing covered information including secure storage, access, transport and disposal

Resources:

Confidentiality Agreement Customer Information/Personally Identifiable Information

Enterprise Risk Management Policy

Family Educational Rights to Privacy Act, 20 USC Section 1232g, 34 CFR Part 99

Academic Catalog, Family Educational Rights to Privacy Act Policy

Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 U.S. Code Section 6801

Information Security Incident Response Plan Policy

Information Technology Acceptable Use Policy

National Institute of Standards and Technology, Special Publication 800-171

Record Retention Policy

Policy Contacts:

Name	Contact Information
Zachary Lewis, AVP IT	Zachary.Lewis@uhsp.edu; 314-446-8402
Eric Knoll, Vice President, Operations & Chief Compliance Officer	Eric.Knoll@uhsp.edu; 314-446-8375