ST. LOUIS COLLEGE of PHARMACY

Information Technology
Data Protection Standards - Data Protection Requirements

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

Faculty , Staff , Students , Contractors_Vendors

Policy Overview:

Issued: 11-30-2018

Next Review Date: 03-07-2023

Frequency of Review: Annually

This Guideline complements the Data Classification Policy by defining (1) the requirements for handling and protecting information at each stage of its lifecycle from creation to destruction and (2) the minimum security standards required for any electronic device that may be used to access or store Sensitive Information owned or used by University of Health Sciences and Pharmacy.

Sensitive Information is University Data that is classified as Internal, Confidential, or Restricted Use. See the Data Classification Policy for definitions and examples of each of these classifications.

Public (non-Sensitive) Information does not require any level of protection from disclosure but appropriate precautions should be taken to protect original (source) documents from unauthorized modification.

Applies to all active members of the University community, including faculty, students, staff, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access, and to those who register their computers and other devices through Conference and Event Services programs or through other offices, for use of the campus network.

Details:

The data handling protections outlined in this document apply to all Sensitive Information, both physical and electronic, throughout all the University of Health Sciences and Pharmacy.

Information Lifecycle

The information lifecycle is the progression of stages or states in which a piece of information may exist between its original creation and final destruction. These phases are: Collecting, Accessing, Sharing, Sending, Storing, Auditing, Incident Reporting and Destroying.

It is important to understand that Storing refers to a broad spectrum of activities including putting a file in a filing cabinet or on to a file server or entering information into a database or spreadsheet. The requirements for Storing information apply equally to the source and to any copies made. For example, when a file is downloaded or copied from a file server to a laptop computer for use offline, it is Stored in that new location and all of the Storing requirements must be followed.

For information about data retention, refer to the Record Retention Policy.

Requirements for Protection

Each classification of data has different requirements for protection throughout the lifecycle of use. The requirements for each *Internal Data*, *Confidential Data, & Restricted Use Data* are detailed below.

Roles

Central
Information Technology Department is responsible for providing consulting and training concerning security, maintaining the security of the central network, a central secure email service, and providing resources for implementing and supporting encryption technologies.

Departmental
Each department and organization, led by a Data Security Administrator (DSA) or other designee, is responsible for complying with these requirements, including helping their personnel understand the classification of the information that they work with and for providing or referring people to appropriate resources to ensure that information is protected in accordance with this policy.

Departments and organizations within the University should, as appropriate, take advantage of centralized services available to support the requirements of this policy. There are areas where the University benefits from standardization or economies of scale by the deployment of enterprise processes or solutions.

Personal
UHSP personnel are responsible for complying with all UHSP policies, including this one, to the best of their understanding and to make reasonable efforts to properly understand.

Procedures:

Internal Data

Collecting	No restrictions.	
Accessing	Access should be provided as required for business devices used to access sensitive (non-Public) information must meet minimum security standards. This applies to paper and electronic data.	
Sharing	Share with employees as needed. Share with vendors/third-parties as approved by department head. This applies to paper and electronic data.	
Sending	Paper	Send in a manner that protects the information from incidental or casual reading.
	Electronic	Use a method that requires recipient to authenticate prior to receipt, such as email, a web site that requires Web Login, or a file server that requires a password. Use secure email service for more private data
Storing	Paper	Keep in non-public areas when not in use.
	Electronic	Devices used to store sensitive (non-Public) information must meet minimum security standards.
	Electronic Media (CD, DVD, USB, etc.)	Store media in a non-public location when not in use.
Auditing	ALL	Conduct a periodic review of where this data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols.
Incident Reporting	ALL	Report the loss of any Internal Data to the local department head who will determine the requirements, if any, for further reporting.
Destroying	ALL	Review University Record Retention Policy before disposing of records.
	Paper & Disposable Electronic Media (CDs, DVDs)	For Internal documents with sensitive content, consider shredding materials before disposing of them.
	Electronic Files (Data) Reusable Electronic Storage Devices (USB keys, disk drives)	Use standard operating system utilities to delete files.
	All Electronic Storage Media at End of Life, including Disk Drives	It is best practice to securely erase these devices before disposing of them. See the Media Destruction Policy for more details.

Confidential Data

Collecting	Reduce or eliminate collection where not required for business function. Collection of some types of Confidential data about individuals may require the approval of the appropriate Data Trustee(s). See the Data Management Guide for a list of the trustees and the approval request form.
Accessing	Access to some Confidential data requires approval of a Data Trustee on a per-individual basis. See the Data Management Guide for a

	list of the trustees and the approval request form. Devices used to access sensitive (non-Public) information must meet minimum security standards. Ensure protocols are in place to immediately remove access upon change in employment status of any individual with access.	
Sharing	If you are uncertain if a piece of *Confidential* information should be shared, escalate the request to an appropriate supervisor or Data Trustee. For types of data that are governed by a Data Trustee, this information may be shared only for business purposes and only as approved by the appropriate Data Trustee, except where the information is being given to approved custodians of that type of data. Information concerning a small number of individuals may be shared internally without Trustee review if the recipient of the data has a need-to-know and is entrusted with the same type of information for their job function. Note: Non-disclosure language or a confidentiality agreement may be appropriate. For example: • Grades need to be communicated to the Registrar's office • Faculty may consult with other faculty about a student's performance, as appropriate, and consistent with applicable polices and laws including the Family Educational and Right to Privacy Act. • Sharing information with vendors and third-parties requires Data Trustee approval For types of data that are not governed by a Data Trustee, the information may be shared internally on a need-to-know basis Information may be shared with the subject of the record or with another party with the subject's approval, as appropriate.	
Printing, Copying,& Scanning	Printing, Copying,& Scanning	Printers often store the printed document on a local hard drive, potentially allowing unauthorized access to the information. Avoid printing *Confidential* data unnecessarily.
Sending	Paper	Address to the specific intended party and send in sealed security envelopes. Mark with "For intended recipient only". Outside the University, paper should be sent via certified mail or with an authorized courier.
	Electronic	Particularly sensitive data or large volumes of confidential data should be encrypted during transmission. If confidential information is to be stored on removable media (CD/DVD/USB/External HD) or in the cloud, see the section below regarding the proper storage.
	Fax	Fax machines often store the faxed messages in memory, potentially allowing unauthorized access. Consider alternatives to faxing *Confidential* data where possible. If a fax must be used, consider taking reasonable steps to protect the data, including the use of a cover sheet stating that the fax is *Confidential* and to be read only by the named recipient. Also consider coordinating with the intended recipient so he or she is on hand to directly receive the fax before you begin to send.

	Smart Phones and tablet devices (such as iPads)	The use of smart phones to access Confidential data, such as through email, puts that data at higher risk of unintended disclosure Individuals accessing Confidential Data via their such a device is prohibited.
Storing	Paper	Should be stored in physically secure areas that are accessible only by authorized individuals. The number of copies should be kept to a minimum.
	Electronic	Encryption of stored data is recommended. Devices used to store *Confidential* Information must be UHSP owned devices managed by the IT Department. Cloud services may be used if they have been approved for this purpose by Information Security.
	Electronic Media	Confidential data should only be stored on UHSP owned and managed computers. Preferably on files servers or within approved applications that are backed up.
Auditing	ALL	Each unit or department should conduct periodic reviews of where *Confidential* data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols. Verify that procedures for removing access are documented and accurate.
Incident Reporting	ALL	Any unauthorized disclosure or loss of this information must be reported to the appropriate dean or department head and the UHSP Security Incident Response Team in accordance with the Security Incident Response Policy. Deans and department heads should report significant unauthorized disclosures or losses of *Confidential* data to the Security Incident Response Team. If you are unsure if an incident is significant, contact your department head. (Examples include: A large quantity of information, sensitive personally identifiable information, a stolen/ lost laptop known to contain *Confidential* information, etc.)
Destroying	ALL	Review Record Retention Policy and the information in this destruction section before disposing of records. Do not destroy records that are the subject of a litigation hold or that must be retained pursuant to the University record retention policy.
	Paper & Disposable Electronic Media	Physically destroy using a shredder or similar appropriate technology and then recycle or discard. See

		the Media Destruction Policy for more details.
	Electronic Files (Data)	Delete using an approved secure deletion program. See the Media Destruction Policy for more details.
	All Electronic Storage Media at End of Life, including Disk Drives	Functional electronic media that is erased using a secure erase tool may be recycled or disposed of. Non-functional electronic media (damaged disk drives) must be physically destroyed. See the Media Destruction Policy for more details on both methods.
	Device End of Lease or End of Life (Printers, Copiers, Multi-function office machines)	Devices such as these often contain hard drives which must be properly erased, or “wiped”, prior to leaving UHSP control (returned to the vendor, sent to surplus, donated, disposed of, etc.). For information on how to properly wipe the drive, see the documentation for your device or contact UHSP Information Technology Department.

Restricted Use Data

Collecting	Eliminate collection whenever possible. Collection of *Restricted Use* data about individuals must be approved by and provided to the appropriate Data Trustee(s). See the Data Management Guide for a list of the trustees and the approval request form.	
Accessing	Access to *Restricted Use* data requires approval of a Data Trustee. See the Data Management Guide for a list of the trustees or speak with your department head. Avoid accessing or using *Restricted Use* data whenever possible, and do so from as few different devices as possible. Devices used to access *Restricted Use* information must be security managed by UHSP IT Department for *Restricted Use* information. The custodian of the system or information must immediately remove access from any person that no longer requires that access as part of their job function.	
Sharing	If you are uncertain if a piece of *Restricted Use* information should be shared, escalate the request to an appropriate supervisor or Data Trustee. This information may be shared only for need-to-know business purposes and only as approved by the appropriate Data Trustee, except where the information is being given to approved custodians of that type of data. Information concerning a small number of individuals may be shared internally without Trustee review if the recipient of the data has a need-to-know and is entrusted with the same type of information for their job function. Note: Non-disclosure and other types of agreements (business associate agreements) may be necessary. Such agreements or agreement forms must be approved by General Counsel. For example: • A pharmacist may consult with another pharmacist regarding a patient’s case, where appropriate. • Sharing information with vendors and third-parties requires Data Trustee approval and a review by UHSP Information Security who may consult with General Counsel and/or the CISO. Information may be shared with the subject of the record or with another party with the subject’s approval, as appropriate.	
Printing, Copying,& Scanning	Printing, Copying, & Scanning	Printers often store the printed document on a local hard drive, potentially allowing unauthorized access to the information. Avoid

		printing *Restricted Use* data unnecessarily.
Sending	Paper	Address to the specific intended party and send in sealed security envelopes. Mark with “For intended recipient only”. Outside the University, paper must be sent via certified mail or with an authorized courier.
	Electronic	Data is required to be encrypted during transmission. If *Restricted Use* data must be placed on removable media (CD/DVD/USB/ External HD) or in the cloud, it must be properly protected. Consult with the IT Department if you have questions about the transport security of your information. Compensating controls must be formally documented and an exception approved by Information Security where this is not technically possible.
	Fax	Fax machines often store the faxed messages in memory, potentially allowing unauthorized access. Avoid faxing *Restricted Use* data where possible. If a fax must be used, include a cover sheet stating that the fax is *Restricted Use* and to be read only by the named recipient. Also, coordinate with the intended recipient so he or she is on hand to directly receive the fax before you begin to send.
	Smart Phones and tablet devices (such as iPads)	These devices must not be used to access Restricted Use Data.
Storing	Paper	Keep in locked filing cabinets in physically secure areas that are accessible only by authorized individuals. Keep the number of copies of the data to a minimum.
	Electronic	Encryption of stored data is required. Devices used to store sensitive (non-Public) information must meet minimum security standards. Cloud services may not be used to process or store *Restricted Use* data unless they have been approved for such use by Information Security and the appropriate Data Trustee.
	Electronic Media	Encryption of stored data is required. Store media in a secure location when not in use. Media should be inventoried upon creation and destroyed as soon as it is no longer needed.
Auditing	ALL	Each unit or department must conduct periodic reviews of where *Restricted Use* data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols. Verify that procedures for removing

		access are documented and accurate.
Incident Reporting	ALL	Any unauthorized disclosure or loss of this information must be reported to the appropriate dean or department head and the UHSP Security Incident Response Team in accordance with the Security Incident Response Policy. Deans and department heads should report significant unauthorized disclosures or losses of *Confidential* data to the Security Incident Response Team. If you are unsure if an incident is significant, contact your department head. (Examples include: A large quantity of information, sensitive personally identifiable information, a stolen/ lost laptop known to contain *Confidential* information, etc.)
Destroying	ALL	Review University Record Retention Policy and the information in this destruction section before disposing of records. Do not destroy records that are the subject of a litigation hold or that must be retained pursuant to the University record retention policy.
	Paper & Disposable Electronic Media (CDs, DVDs)	Physically destroy using a cross-cut shredder or similar appropriate technology and then recycle or discard. See the Media Destruction Policy for more details.
	Electronic Files (Data)	Delete using an approved secure deletion program. See the Media Destruction Policy for more details.
	All Electronic Storage Media at End of Life, including Disk Drives	Functional electronic media that can be overwritten using a secure erase tool then may be recycled or disposed of. Non-functional electronic media (damaged disk drives) must be physically destroyed. See the Media Destruction page for more details.
	Device End of Lease or End of Life (Printers, Copiers, Multi-function office machines)	Devices such as these often contain hard drives which must be properly erased, or “wiped”, prior to leaving UHSP control (returned to the vendor, sent to surplus, donated, disposed of, etc.). For information on how to properly wipe the drive, see the documentation for your device or contact UHSP Information Technology Department.

Media Destruction One-Sheets

Federal and state law or University policy may require that information is retained for a certain period of time. For information on the required retention periods, see University Record Retention Policy. However, it is just as important to remove and properly destroy such information when the retention period is over.

UHSP Information Security maintains reference sheets regarding the proper destruction of Sensitive Information when it reaches the end of its retention period. These reference sheets also provide instructions on the proper destruction or cleaning of media on which sensitive information is stored.

Please refer to the Media Destruction Policy and/or the Record Retention Policy for more information on this important topic.

Exceptions
UHSP Information Security is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and will be based on the implementation of appropriate compensating controls.

Important
Failure to comply with the Data Protection Standards may result in harm to individuals, organizations or UHSP. The unauthorized or unacceptable use of University Data, including the failure to comply with these standards, constitutes a violation of University policy and may subject the User to revocation of the privilege to use University Data or Information Technology or disciplinary action, up to and including termination of employment.

Responsibilities:

Position/Office/Department	Responsibility
All computer and infrastructure users	Abide by Data Protection Requirements

Resources:

Data Protection Standards policies

Digital Millennium Copyright Act Policy

Minimum Security Standards

College Record Retention Policy

Media Destruction Policy

Security Incident Response Policy

Policy Contacts:

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