Data Classification & Handling Guide

There are four classification levels of institutional data at the University of Kansas. To ensure proper handling and sharing of data, please use the following classification levels. Data classifications are listed below starting with the most sensitive to least sensitive:

Critical

Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access. Access will typically be granted on a case-by-case basis to a very small group of individuals. This data must be encrypted while being stored or transmitted.

Restricted

Because of legal, ethical, or other constraints, this data requires authorization to be accessed. Access will typically be granted by job or system access roles. It is recommended that this data is encrypted while being stored or transmitted.

Internal

This data may be accessed by employees of the university for purposes of university business.

Public

Few restrictions are placed on this data and it is generally released to a member of the public upon formal request. Employees must consult the “Releasing Information to Third Parties” policy prior to releasing any data to a member of the public.

Data Classification Examples

Critical:

- Protected Health Information (HIPAA) and health insurance policy ID numbers *
- FERPA - student data including but not limited to grades, exams, rosters, official correspondence, financial aid, scholarship records, enrollment, etc
- Data subject to the Children's Online Privacy Protection Act (COPPA) - information collected from children under the age of 13
- Student Loan Application Information (GLBA)
- Financial account numbers (bank account, investment account, P-card, etc)
- Credit card/E-Commerce data (PCI) – This data should NEVER be stored. Departments wishing to accept credit cards should contact the E-Commerce committee by visiting https://ecommerce.ku.edu
- Attorney-client privileged information
- Data subject to Defense Federal Acquisition Regulation Supplement (DFARS) or Federal Acquisition (FAR) requirements
- Export controlled information--International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)
- Passwords/PINs
- Personally Identifiable Information (PII) including SSN, passport numbers, visa numbers,other national ID numbers, driver's license numbers
- Audit working papers
- Biometric identifiers, including finger and voice prints
- Other data covered by federal and/or state confidentiality laws
- Criminal Justice Information (KCJIS)
- Tax information (W-2, W-4, 1099, etc)
- Sensitive identifiable human subject research data *

Restricted:

- Donor/prospect contact information and non-public gift information
- Audit reports
- Individually identifiable data on race, color, ethnicity, religion, sex, national origin, age, ancestry, disability, status as a veteran, sexual orientation, marital status, parental status, gender identity, gender expression and genetic information
- Competitive business information
- Faculty/staff employment applications, personnel files, benefits, birth date, personal contact information
- Location data for devices connected to KU wired and wireless networks
- Data subject to non-disclosure agreements
- Conflict of Interest disclosures
- Bulk email addresses

Internal:

- Salary information
- Student and employee ID numbers
- Engineering, design, and operational information regarding KU facilities and infrastructure
- Non-public policies and policy manuals
- Unpublished grant proposals, research data, manuscripts and associated correspondence that are not subject to other confidentiality requirements (at data owner's discretion)
- Summarized data on race, color, ethnicity, religion, sex, national origin, age, ancestry, disability, status as a veteran, sexual orientation, marital status, parental status, gender identity, gender expression and genetic information
- Budgetary information, University planning information
- Non-public financial and procurement information

Public:

- FERPA Directory Information (http://policy.ku.edu/registrar/student-record-policy)
- Information authorized to be available on or through KU websites without KU Online ID authentication
- Public policies and procedure manuals
- Course offerings
- Annual reports
- Job postings

* Please refer to the Data Classifications Definitions for more information

Data Classification Definitions

Under HIPAA (Health Insurance Portability and Accountability Act), PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual

PHI is individually identifiable health information that relates to the:

- Past, present, or future physical or mental health or condition of an individual
- Provision of health to the individual by a covered entity (for example, hospital or doctor)
- Past, present, or future payments for the provision of health care to the individual

---

Sensitive Identifiable Health Subject Research

Individually identifiable research data containing sensitive information about human subjects. A human subject is a living individual about whom a researcher obtains data and information that can be used to identify him or her. The researcher determines whether that data is sensitive or not, based on privacy and ethical considerations. This data type is governed by the Federal Policy for the Protection of Human Subjects (also called the "Common Rule"). Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data. That includes illegal behaviors, drug or alcohol abuse, sexual behavior, mental health or other sensitive health or genetic information, and any data collected under a National Institutes of Health (NIH) Certificate of Confidentiality. A Data Use Agreement may define additional constraints on the handling of a covered data set.

Data Handling Guideline

✓ = Yes ⊘ = No P = Permission can be granted by the KU IT Security Office

Storage Platform	Critical	Restricted	Internal	Public	Notes
One Drive for Business	P	✓	✓	✓	
Team sites/SharePoint	P	P	✓	✓	
CFS/ResFS	⊘	✓	✓	✓	Critical and Restricted data should not be stored on standard CFS/ResFS shares.
Cat1 CFS/ResFS	✓	✓	✓	⊘	
KU IT managed device (computers, tablets, phones)	✓	✓	✓	✓	
KU owned but unmanaged device	⊘	✓	✓	✓	
Personal devices (computers, tablets, phones)	⊘	⊘	✓	✓	Only public data can be stored on unmanaged devices.
Portable storage devices regardless of ownership (external hard drives, thumb drives, etc)	⊘	⊘	✓	✓	Only public data can be stored on unmanaged devices.
Personal cloud storage (Dropbox, Box, OneDrive, Google Drive etc)	⊘	⊘	⊘	✓	Only public data can be stored on personal cloud storage.
Cloud hosting platforms managed by KU IT (Amazon AWS, Microsoft Azure, etc)	⊘	✓	✓	✓	
Cloud hosting platforms not managed by KU IT (Amazon AWS, Microsoft Azure, etc)	⊘	⊘	⊘	✓	Only public data can be stored on cloud platforms not managed by KU IT.
KU IT managed content management systems (Drupal, WordPress, cPanel sites)	⊘	⊘	✓	✓	Only public and internal data may be stored or transmitted with approval of the KU IT Security Office.
Web hosting providers (Weebly, Squarespace, etc), photo hosting services (Flickr, Google Photos), streaming video services (YouTube, Twitch, etc)	⊘	⊘	⊘	✓	Only public data can be stored or transmitted using 3rd party web hosting providers or photo hosting/video steaming services.
Social media sites (Facebook, LinkedIn, Instagram, Twitter, etc), 3rd party chat services (Slack, Discord, etc)	⊘	⊘	⊘	✓	Only public data can be stored or transmitted using social media platforms or 3rd party chat services of any kind.
KU enterprise systems (HR Pay, Enroll & Pay, Blackboard)	✓	✓	✓	✓	Contact the appropriate data owner for assistance with data you may need to store or access on these systems.
KU IT managed e-mail (O365 or on-premises)	P	✓	✓	✓	
Email systems not managed by KU IT (departmental email, Gmail, Yahoo, Hotmail, etc)	⊘	⊘	⊘	✓	Only public data may be stored or transmitted using departmental email systems or personal email accounts.
KU survey platforms (Qualtrics, REDCap)	P	✓	✓	✓	
Non-KU managed survey/calendaring platforms (SurveyMonkey, Calendly, Doodle, etc)	⊘	⊘	⊘	✓	Only public data may be collected or stored using non-KU managed survey/calendaring platforms.
Email marketing services (Constant Contact, MailChimp, etc)	⊘	⊘	⊘	✓	Only public data may be stored or transmitted using email marketing services, whether or not they are paid for with KU funds.