Sensitive Data – Reference Examples and Regulations

Sensitive Data - Any confidential or proprietary information not routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy. Unauthorized access to sensitive information may result in an invasion of privacy, may expose the University to financial risk, or result in negative impacts on the operations, or reputation of the University.

Medical and health records (protected health information for covered entities) *Health Insurance Portability and Accountability Act of 1996 - HIPAA*

Any identifier *in combination* with health information (i.e., date on vial of blood, emplID and BP)

(1) Names (including initials)
(2) Street address, city, county, precinct, zip code, and equivalent geo-codes
(3) **ALL** elements of dates (except year) for dates directly related to an individual and all ages over 89 **(this would include procedure dates, date of admission, date of lab work, etc.)**
(4) Telephone numbers
(5) Fax numbers
(6) Electronic mail addresses
(7) Social security numbers
(8) Medical record numbers
(9) Health plan ID numbers
(10) Account numbers
(11) Certificate/license numbers
(12) Vehicle identifiers and serial numbers, including license plate numbers
(13) Device identifiers/serial numbers
(14) Web addresses (URLs)
(15) Internet IP addresses
(16) Biometric identifiers, incl. finger and voice prints
(17) Full face photographic images and any comparable images
(18) Any other unique identifying number, characteristic, or code

Student Grades and other enrollment information – (student education records – all schools receiving funds under US Dept. of Education Programs *Family Educational Rights and Privacy Act – FERPA*

(1) personal information (student or parent or family member name, address, identifier such as social security number or student number, personal characteristics or other information that would make the student's identity easily traceable)
(2) enrollment records
(3) grades

(4) schedules

FERPA is clear that the requirement is “stand alone.” If any data/information could be used to identify a student then it must be protected.

*Not included: “directory” information such as name, address, telephone number, date (month and day) and place of birth, degrees, honors and awards, and dates of attendance *unless* requested inclusion by student or parent

*Record information can be shared with the following, without consent:
School officials with legitimate educational interest Other
schools to which the student is transferring
Specified officials for audit or evaluation purposes
Appropriate parties in connection with financial aid to a student
Organizations conducting certain studies for or on behalf of the school Accrediting
organization
In compliance with a judicial order or lawfully issued subpoena
Appropriate officials in cases of health and safety emergencies
State and local authorities, within a juvenile justice system, pursuant to specific state law

Credit Card Data
Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS is a baseline of technical and operational requirements set forth by the PCI Security Standards Council designed to protect cardholder data. The PCI Security Standards Council was founded by the five payment brands. Non-compliance penalties are carried out by the individual payment brands.

PCI DSS applies to all entities involved in payment card processing – including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data as defined below:

Account Data	Sensitive Authentication Data
Primary Account Number (PAN)	Full track data (magnetic-strip data or ‘chip’)
Cardholder Name	CAV2/CVC2/CVV2/CID
Expiration Date	PINs/PIN blocks
Service Code	

University policy prohibits obtaining or transmitting credit card information via email and the storage of card information on devices not deemed PCI compliant.

Bank Account and other Financial Information and o*ther personally identifiable information* *Kentucky House Bill 5*

"An **agency** or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of form in which the **personal information** is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to protect and safeguard against **security breaches**"

Agency -"every public institution of postsecondary education, including every public university in the Commonwealth of Kentucky and public college of the entire Kentucky Community & Technical College.."

Security breach – "unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of unencrypted or unredacted records or data that compromises … or reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm …."

Personal Information – Individual's first name (or first initial) and last name; personal mark, unique biometric or genetic print or image in combination with one or more of the following:

(1) Account number, credit or debit card number, that in combination with a security code, access code or password would permit access to an account
(2) Social Security number
(3) Tax payer ID that incorporates SSN
(4) Driver's license number, state ID card number or other individual id issued by any agency: - EMPLID
(5) Passport number or other ID number issued by US government
(6) Individually identifiable health information as defined in 45 CFR 160.103 except for educational record covered by FERPA

University Policy/Other – can provide personally identifiable information or damage

(1) Dates of birth (in combination with name, address and/or phone number)
(2) User ID and passwords (in combination)
(3) Grant reviews, restricted research information
(4) Information restricted by contract

*Any confidential or proprietary information not routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy.