I. PURPOSE

To ensure that UK complies with all federal, state and local laws and regulations as well as with all University regulations and policies, all data and information shall be classified to indicate the need, priorities and business value which, in turn, can be used to determine the expected degree of protection when handling the information. In other words, once classified, decisions can be made concerning data/information release, sharing, handling and management as well as deciding the most appropriate and reasonable means of protecting it via administrative, technical and physical safeguards, given its use and context.

II. APPLICABILITY

This policy is applicable to all personnel who own UK data, managed UK information assets, or have UK-data custodial or stewardship responsibilities (i.e., Data Owners, Data Custodians, and Data Stewards.)

This policy applies to all data created or used by UK in meeting its mission (i.e. any data used by any UK units regardless of their academic, healthcare, research or and administrative purpose and regardless if it is considered to be a public record must be classified.)

This policy also applies to, but is not limited to, data/information that is created, stored or shared via any means. This includes electronic data, data or information on paper, and data/information shared orally or visually (such as telephone and video conferencing).

III. POLICY

All UK data shall be classified based upon risk and business value. The classification of data shall take into account legal and regulatory obligations of the university, contractual agreements, the risk and cost of unauthorized access, and the strategic or proprietary worth of the data.

Classification Levels

All data shall be classified into one of three categories. These three categories are as follows:

1. Confidential,
2. Sensitive, or
3. Public.
1. Confidential

- Confidential is the highest level of sensitivity.
- Confidential data require the highest level of protection.
- Confidential data and confidential information are
  a) usually concerning people\(^1\) or critical University/business functions,
  b) required by regulatory or legal requirements\(^2\) to have special handling measures, and
  c) not for public disclosure.

- Data/information that shall be classified as “confidential” and, as such, require a high
duty of care and a high level of protection from risk and disclosure include, but are not
limited to the following:
  a) **Protected Health Information** (PHI)\(^1\) as identified by the Health Insurance
    Portability and Accountability Act (Public Law 104-191 as amended, aka “HIPAA”),
    specifically as defined by the Code of Federal Regulations 45 CFR. 160.103,
  b) **Education records**\(^2\) as identified by the Family Educational Rights and Privacy Act
    (20 USC § 1232g; 34 CFR Part 99, aka “FERPA”),
  c) **Personally identifiable information** (PII) as identified by Kentucky Revised
    Statutes (KRS 61.878(5) and KRS 61.931(6)(a), aka “House Bill 5”, the Personal Information
    Security and Breach Investigation Procedures and Practices Act (i.e., Kentucky’s data breach
    notification law”),
  d) A credit card’s **Primary Account Number**\(^4\) (aka “PAN”) as identified by the
    Payment Card Industry Security Services Council’s Data Security Standard (PCI
    DSS), and
  e) **Nonpublic personal (financial) information** as identified by Section 509(4) of the
    Financial Services Modernization Act of 1999 (Public Law 106–102, 113 Stat. 1338, 15
    USC § 6801-6810; aka The Gramm-Leach-Bliley Act or GLBA\(^5\)).

Examples of “confidential” data and information include, but are not limited to, the following:
1. Medical care information, patient names, patient contact information, and human subject
   information,
2. Biometric identifiers and demographic information that can, in turn, be used to identify otherwise-
   protected healthcare information,
3. Student data and educational records other than those deemed “directory information” by UK
   Legal and the UK Registrar, and
4. Social Security Numbers, Bank Account Numbers, Credit Card Numbers, Driver’s License
   Numbers, and student/parental financials.

---

\(^1\) Data/information concerning people that can, in turn, be used to commit fraud (Identity Theft) and larceny (i.e., Social
Security Number, Bank Account Number, etc.).

\(^2\) See End Notes.
2. **Sensitive**

- Data and information that are classified as “sensitive” do not meet the requirements of “confidential” data but nonetheless, require a moderate level of protection from risk and disclosure.

- Data and information shall be classified as “sensitive” if their unauthorized disclosure or inappropriate use could adversely impact any aspect of the University of Kentucky, students, employees, patients or affiliates but would not necessarily violate laws or regulations.

Examples of “sensitive” data and information include, but are not limited to, the following:

1. Incomplete or unpublished research,
2. Internal memos or reports,
3. Employee data such as UK person ID numbers, personal phone numbers, birth dates and addresses,
4. Data covered by non-disclosure agreements, and
5. Privileged data and documents such as Patient Safety Work Product (PSWP), data covered by attorney-client privilege, and data generated by any UK unit in anticipation of litigation.
3. **Public**

- Data or information that must be made available to the general public shall be classified as “public.”
- Data and information shall be classified as “public” if there are no existing federal, state or University restrictions on access or usage.
- “Public” data and information shall be available to all individuals and entities both internal and external to UK; however, such data and information may still be subject to UK disclosure policies and procedures.
- While the requirements for protection of public data/information are less stringent than that of “confidential” and “sensitive” data, **sufficient controls and safeguards must be maintained**, nonetheless, to ensure the integrity of the data/information and protect against its unauthorized modification or destruction.

Examples of “public” data and information include, but are not limited to:

1. Data on websites intended for the general public,
2. Press releases,
3. Marketing brochures,
4. University and Hospital maps, and
5. Annual reports.
**Data Loss or Security Breach**

The loss of any confidential data, the unauthorized access to any confidential data, and the breach of security to any UK information asset must be reported as soon as possible to one of the following offices:

1. The Office of Corporate Compliance (within UK HealthCare),
2. The UK HealthCare IT Help Desk, or
3. The UK Analytics and Technology (UKAT) Service Desk.

The theft or loss of any computing device containing any confidential data or through which confidential data can be accessed shall also be reported to UK Police.

The appropriate UK accounting departments shall then be notified of the loss of any UK capital asset (i.e., laptop computer, desktop computer, UK-owned smart phone, etc.).

**Data or Information Asset Disposal**

Any information asset containing non-public data/information, when no longer required by regulations to be retained, shall be disposed of through the most appropriate means per UK HealthCare policy [A13-050, Transfer and Disposal of Electronic Media](#) or [UK Treasurer’s Property Disposition Policy](#).

**IV. DEFINITIONS (not complete)**

DATA OWNER refers to a member of UK management who is ultimately responsible and accountable for a specific business unit, business service, College, or UK unit. This role is normally assigned to the senior level manager within the business unit where the data was created. S/he may or may not be the primary user of that asset. The data owner is person who is ultimately responsible for the safeguarding and use of the data. This responsibility extends to classifying the data; however, the responsibility for classifying and safeguarding the data can be delegated. Unless the duties are performed by the data owner, the data owner is also responsible for designating a data custodian (aka “data steward”).

DATA CUSTODIAN (aka “data steward”) refers to the authorized UK employee that has operational-level responsibilities for a specific business unit, business service, College, or UK unit. The data custodian is typically designated by the data owner.

The data custodian is the “steward of the data” for the data owner. Data custodians are responsible for data access, data safeguards and policy implementation.

The identification of the custodians must be explicit since the lack of clear data/information management responsibility may result in poor or non-existent safeguards.
V. REFERENCES

VI. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Primary Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/18/14</td>
<td>Initial draft developed</td>
<td>M. Carr</td>
</tr>
</tbody>
</table>
VII. END NOTES

1. HIPAA defines Protected Health Information (PHI) as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103). The definition exempts a small number of categories of individually identifiable health information, such as individually identifiable health information:

   a) found in employment records held by a covered entity in its role as an employer;
   b) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
   c) or pertaining to a person who has been deceased for more than 50 years.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   i) That identifies the individual; or
   ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

2. FERPA defines education records as those records, files, documents, and other materials which:

(1) Contain information directly related to a student; and
(2) Are maintained by an educational agency or institution or by a party acting for the agency of institution.

There are exceptions - one being institutionally-defined “Directory Information” (see www.uky.edu/registrar/FERPA-privacy).

3. Kentucky’s data breach notification law defines personal information as an individual’s first name (or first initial) and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

   a) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
   b) A Social Security number;
   c) A taxpayer identification number that incorporates a Social Security number;
   d) A driver’s license number, state identification card number, or other individual identification number issued by any agency;
   e) A passport number or other identification number issued by the United States government; or
   f) Individually identifiable health information as defined in 45 CFR § 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g


5. GLBA defines “nonpublic personal information” to mean “personally identifiable financial information” that is provided by a consumer to a financial institution (including Universities in their capacity to make loans), results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution.

Examples of personally identifiable financial information include the following:

   a) Information a consumer provides on an application to obtain a loan, credit card, or other financial product or service; or
   b) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

6. Patient Safety Work Product (PSWP) is the data/information protected by the privilege and confidentiality protections of the Patient Safety and Quality Improvement Act of 2005 (Public Law 109-41) and the Patient Safety Rule (43 CFR Part 3).