I. PURPOSE

The purpose of this policy is to assist every UK unit meet its commitment to comply with all data safeguarding and privacy provisions of every federal, state and local law and regulation that applies to it.

This policy lists the federal, state and local laws and regulations that apply to most, in not all, UK units. It requires units that have compliance requirements in addition to those listed herein to document them and document the safeguards (or compensating controls) that are implemented to ensure compliance.

II. APPLICABILITY

This policy is applicable to all UK units and 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.)

III. POLICY

Every UK unit and employee shall comply with the following federal, state and local laws and regulations:

   a) The Health Insurance Portability and Accountability Act (Public Law 104-191 as amended, aka “HIPAA”) with special attention to the safeguarding of Protected Health Information (PHI) as identified by specifically as defined by the Code of Federal Regulations 45 CFR. 160.103,

   b) The Family Educational Rights and Privacy Act (20 USC § 1232g; 34 CFR Part 99, aka “FERPA”) with special attention to the safeguarding of Education recordsii,

   a) the Personal Information Security and Breach Investigation Procedures and Practices Act (aka “House Bill 5”, Kentucky’s data breach notification law) with special attention to the safeguarding of personally identifiable information (PII) as identified by Kentucky Revised Statutes (KRS 61.878(5) and KRS 61.931(6)(a), iii),

   b) The Payment Card Industry Security Services Council’s Data Security Standard (PCI DSS) with special attention to the safeguarding of a credit card’s Primary Account Numberiv (aka “PAN”) as identified by, and

   c) 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) with special attention to safeguarding nonpublic personal (financial) information as identified by Section 509(4).

If a UK unit is required to comply with additional laws and regulations, the unit shall document them and document the safeguards (or compensating controls) that are implemented to ensure compliance.
IV. DEFINITIONS  *(not complete)*

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>

(Additional content may be present in sections not fully visible in the image.)
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) 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;