

**SUMMARY OF SELECTED FEDERAL LAWS AND REGULATIONS ADDRESSING CONFIDENTIALITY, PRIVACY AND SECURITY (5/28/2015)**

State Law	Citation	General Description	Applicability	Information Covered	Summary
Personal Information Security and Breach Investigation Procedures and Practices Act	KRS 61.931, et seq.		Every state agency, including KDE, every public school district, every local education agency, and every entity with which the preceding agencies/institutions have contracts, including memorandums of understanding (MOUs).		<p>The Personal Information Security and Breach Investigation Procedures and Practices Act</p> <p>This Act concerns the protection of personal information requiring:</p> <ol style="list-style-type: none"> <li>1. Procedures and practices to safeguard against security breaches must be implemented by any entity that maintains or possesses personal information in accordance with applicable KRS and federal laws.</li> <li>2. For any contracts (MOUs) involving personal information that are entered into or amended after Jan. 1, 2015, specific language requiring protection of the data must be included.</li> <li>3. For any suspected or confirmed breach, the appropriate agency contacts must be notified and</li> <li>4. Within 72 hours of a suspected or confirmed breach, notify, via the FAC-001 form (See appendix ___), the appropriate agency contacts (See appendix ___.) and begin conducting a “reasonable and prompt” investigation to determine “whether the security breach has resulted in or is likely to result in the misuse of personal information.”</li> <li>5. Within 48 hours of completion of the investigation, notify the appropriate staff contacts referenced in Item c. above if the investigation finds that the misuse of personal information has occurred or is likely to occur.</li> <li>6. Within 35 days of suspected or confirmed breach, notify all individuals impacted by the breach in a manner required by the Act.</li> <li>7. If the investigation determines that misuse of personal information has not occurred or is not likely to occur, notification of the impacted individuals is not required, but records of the decision and evidence must be kept. Notification of the agency contacts, above, is still required noting that misuse of personal information has not occurred.</li> </ol>

**Disclaimer:** This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.

**SUMMARY OF SELECTED FEDERAL LAWS AND REGULATIONS ADDRESSING CONFIDENTIALITY, PRIVACY AND SECURITY (5/28/2015)**

State Law	Citation	General Description	Applicability	Information Covered	Summary
<b>Personal Data Security</b>	HB 341 (KRS___)		to KDE and school districts	restricted personal information	Provides general guidelines and recommendations related to measures to protect and prevent the access to restricted personal information by any person that does not have the proper access rights, authority or the "need to know, and protocols in regards to notifying any affected individual should this type of information be made available in paper or electronic form to any unauthorized person.
<b>Kentucky Family Education Rights and Privacy Act</b>					
<b>The Privacy Act of 1974</b>	5 U.S.C. § 552a; 45 C.F.R. Parts 5b; OMB Circular No. A-108 (1975)	The Privacy Act of 1974 is a withholding statute.	Any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency	The Privacy Act applies when the federal government maintains a system of records by which information about individuals is retrieved by use of the individuals' personal identifiers (names, social security numbers, or any other codes or identifiers that are assigned to the individual). A "record" for purposes of the Privacy Act means any item, collection, or grouping of information about an individual that is maintained by the agency and that contains the individual's name or other personal identifier.	The Privacy Act of 1974 and its implementing regulations:  1) Prohibits the disclosure of personally identifiable information maintained by agencies is a system of records without the consent of the subject individual, subject to twelve codified exceptions  (2) Grants individuals increased rights of <u>access</u> to agency records maintained on themselves.  (3) Grant individuals the right to seek <u>amendment</u> of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.  (4) Establishes a code of " <u>fair information practices</u> " which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

**Disclaimer:** This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.

**SUMMARY OF SELECTED FEDERAL LAWS AND REGULATIONS ADDRESSING CONFIDENTIALITY, PRIVACY AND SECURITY (5/28/2015)**

State Law	Citation	General Description	Applicability	Information Covered	Summary
Health Breach Notification Rule (Federal Trade Commission Rule) <a href="#">??Check on this</a>	16 C.F.R. Part 318  <a href="http://www.ftc.gov/oss/2009/04/R911002/healthbreach.pdf">http://www.ftc.gov/oss/2009/04/R911002/healthbreach.pdf</a>	This proposed rule requires vendors of personal health records (PHRs) and related entities to notify individuals when their individually identifiable health information is breached	Vendors of PHRs, their related entities, and other third party service providers who do not qualify as entities covered under HIPAA	Unsecured identifiable health information of an individual in a personal health record	These proposed rule requires vendors of personal health records (PHRs) and related entities to provide notice to consumers following a security breach. Stipulates that if a service provider of a PHR vendor experiences a breach, it must notify the PHR vendor. The PHR vendor, in turn, must notify consumers of the breach. The proposed rule contains additional requirements governing the standard for what triggers the notice, as well as the timing, method, and content of notice.
Individuals with Disabilities Education Improvement Act (2004)	20 U.S.C. § 1400, et seq.  34 C.F.R. Parts 300 and 301 <a href="http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=81055712322+1+0+0&amp;WAISaction=retrieve">http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=81055712322+1+0+0&amp;WAISaction=retrieve</a>	Ensure services to children with disabilities	All public and private schools receiving federal funds	Educational records	Governs how states and public agencies provide early intervention, special education and related services to children with disabilities; infants, toddlers, children and youth with disabilities. Includes requirements regarding surrogate parents, notice and parental consent regarding disability information.
Family Educational Rights and Privacy Act (1974)	20 U.S.C. § 1232g  34 C.F.R. Part 99  <a href="http://www.ed.gov/policy/gen/reg/ferpa/index.html">http://www.ed.gov/policy/gen/reg/ferpa/index.html</a>	Privacy of student education records	Educational agencies and institutions that receive funds under any program administered by the Secretary of Education	Educational records maintained by the institution that relate directly to the student	Limits disclosure of educational records maintained by agencies and institutions that receive federal funding. Protects the confidentiality of student records to some extent, while also giving students the right to review their own records. "Directory information" is not protected.
Protection of Pupil Rights Amendment (2002)	20 U.S.C. § 1232h  34 C.F.R. Part 98 <a href="http://www4.law.cornell.edu/uscode/20/1232h.html">http://www4.law.cornell.edu/uscode/20/1232h.html</a>	Protects rights of parents and students	Programs with funding from the U.S. Department of Education	Personal information, including some health related information	Protects the rights of parents and students by 1) making instructional materials used in Department of Education funded surveys and analyses available to parents, and 2) ensuring that written parental consent is obtained before minor students participate in such surveys and analyses. Topics emphasized are: mental and psychological problems; sex behavior and attitudes; illegal, anti-social, self-incriminating and demeaning behavior; and income. Parents or students who believe their rights under PPRA may have been violated may file a complaint with the Department of Education.

**Disclaimer:** This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.

**SUMMARY OF SELECTED FEDERAL LAWS AND REGULATIONS ADDRESSING CONFIDENTIALITY, PRIVACY AND SECURITY (5/28/2015)**

State Law	Citation	General Description	Applicability	Information Covered	Summary
Children's Online Privacy Protection Act (1998) and accompanying rule	15 U.S.C. §§ 6501–6506 16 C.F.R. Part 312 <a href="http://www.ftc.gov/ocs/1999/10/64fr59888.htm">http://www.ftc.gov/ocs/1999/10/64fr59888.htm</a>	Protects children's personal information online	Commercial web sites and other online services directed at children under 13, or which collect users' age r	Personal information	Protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users.
REAL ID Act (2005)	H.R. 1268, 109 P.L. 13	Requires states to implement new requirements for drivers licenses and identification cards	State governments	Personal information	Imposes specific federal driver's license standards. The standards govern what information must be collected for and on the license, and in what format. Requires use of enhanced data collection, automation and security protections. States must meet requirements related to: <ul style="list-style-type: none"> <li>• information and security features for the cards</li> <li>• proof of identity and U.S. legal status</li> <li>• verification of the source documents provided</li> </ul> Also requires each state to share its motor vehicle database with all other states.

DRAFT

**Disclaimer:** This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.