Student Data Privacy Act; SB 367

SB 367 creates the Student Data Privacy Act (Act), which provides restrictions on what data contained in a student's educational record can be disclosed and to whom it may be disclosed. The bill requires that any student data submitted to and maintained by a statewide longitudinal student data system may be disclosed only to individuals or organizations as outlined in the bill.

Under the bill, educational agencies (school districts or the State Department of Education) must give annual written notice that student data may be disclosed as outlined in the Act. The notice must be signed and returned, and the district must keep it on file.

The bill permits student data to be disclosed at any time to the following:

- The student and the student's parent or legal guardian, but only if the data pertain solely to that student;
- Authorized personnel of an educational agency or the Kansas Board of Regents who require such disclosures to perform their assigned duties; and
- Any authorized personnel of any state agency with a data sharing agreement between the state agency and the educational institution.

Authorization is granted for disclosure of student data to any state agency not specified above or to a service provider of a state agency, educational agency or school who performs a specified educational service, provided there is a data-sharing agreement between the relevant educational agency and the state agency or service provider that provides for specific procedures, including data security and destruction or return of the data at the appropriate specified time. (Destruction of data must comply with National Institute of Standards and Technology requirements.) An exception to the data destruction requirement of student transcripts is provided for a service provider that performs an instructional function, if retention of the transcripts is required by applicable laws and rules and regulations.

The bill permits student data to be disclosed to any governmental entity not otherwise specified or to any public or private audit and evaluation or research organization, provided the data disclosed are aggregate and contain no personally identifiable student information. Personally identifiable information may be disclosed if an adult student or a minor student's parent or legal guardian consents in writing. The terms "aggregate data" and "personally identifiable data" are defined in the bill and are exclusive of each other.

In addition, an educational agency is allowed to disclose the following:

- Directory information when the agency deems disclosure is necessary and if consent is given in writing by a student's parent or legal guardian;
- Directory information to such entities as yearbook publishing companies and class ring vendors, including a student's name, address, telephone listing, and other specified information;

- Student data to a postsecondary institution that is required by the postsecondary institution for application or admission;

- Any student data required to comply with a subpoena or court order; and

- Any information required to be disclosed to public health officials for urgent health or safety reasons, in which cases confidentiality requirements apply.

The bill prohibits school districts from collecting biometric data or assessing a student's psychological or emotional state unless written consent is granted. The bill also requires the Department of Education to publish annually on its website a list of the categories of student data that are collected by any statewide longitudinal student data system.

The bill prohibits the administration of any test, questionnaire, survey, or examination containing questions regarding a student's or student's parents' or guardians' beliefs or practices on issues such as sex, family life, morality, or religion, unless permission is requested in writing and granted by a student's parent or guardian. The bill further states that this section does not prohibit school counselors from providing counseling services to a student but does restrict how information obtained through these services may be stored, specifically, by prohibiting the storing of such information on any personal mobile electronic device not owned by the school district.

In the event of a security breach or unauthorized disclosure of personally identifiable student data, the State Board of Education (State Board), local school district board, or any entity having access to the data must notify the subjects of the breach or disclosure and conduct an investigation into the causes and consequences.

The bill grants the Attorney General or any district attorney authority to enforce the first eight sections of the Act.

The bill further requires the State Board to submit a written report to the Governor and the Legislature by May 15, 2015, and each year thereafter, that includes:

- Categories of student data collected;

- Changes to existing data collection, including federal reporting requirements;

- Explanations of any exceptions made related to student data releases; and

- Scope and nature of any privacy or security audits.

Finally, the bill amends the law pertaining to protections for the right of privacy and federal law (KSA 72-6214) by doing the following:

- Requiring the Kansas Board of Regents, the State Board, the board of trustees of any public community college, the board of regents of any municipal university, the governing board of any technical college, and the board of education of any school district to adopt a policy in accordance with the Student Data Privacy Act, in addition to applicable federal laws and regulations to protect the right of privacy for students; and

- Deleting the statement that this section of law controls when there is a conflict between it and any other provision of law.