Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Education Committee

ESSB 5316

Brief Description: Concerning privacy and security of personally identifiable student information.

Sponsors: Senate Committee on Early Learning & K-12 Education (originally sponsored by Senators Dammeier, Rolfes, Rivers, Hasegawa, Brown, Frockt, Dansel, Braun, Chase, Angel and Kohl-Welles).

Brief Summary of Engrossed Substitute Bill

- Increases parent and guardian access to student education records.
- Provides limits to use and disclosure of student-level data, and personally identifiable student-level data (PID).
- Allows directory information to be released in certain circumstances.
- Allows school districts to collect and distribute aggregate data.
- Prohibits collection, retention, or use of biometric information, except for special education purposes.
- Requires the state to develop a data security plan and procedures to safeguard PID, including a model plan for school districts.

Hearing Date: 3/16/15

Staff: Megan Wargacki (786-7194).

Background:

Family Educational Rights and Privacy Act.
The federal Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The FERPA gives parents and eligible students (age 18

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

and older, or attending post-secondary school) certain rights with respect to the student's education records:

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school.
- Parents or eligible students have the right to request that a school correct records that they believe to be inaccurate or misleading.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

Exceptions to the Written Consent Requirement. Under FERPA, personally identifiable information (PII) from a student's education record may not be released without the written consent of the parent or eligible student, with some exceptions. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, e-mail address, date and place of birth, grade level, honors and awards, and dates of attendance, as long as the parent or eligible student has not opted out of this disclosure. In addition, schools may disclose PII from a student's records, without consent, to the following parties or under the following conditions:

- school officials with a legitimate educational interest, including contractors, consultants, and volunteers under certain circumstances;
- other schools to which a 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 organizations;
- to comply with a judicial order or lawfully issued subpoena;
- appropriate officials in cases of health and safety emergencies; and
- state and local authorities, within a juvenile justice system, pursuant to specific state law.

Personally Identifiable Information. The term PII includes:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number, student number, or biometric record;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Biometric Record. The term biometric record, as used in the definition of PII, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

State Law.
Current law provides that the confidentiality of personally identifiable student data must be safeguarded consistent with the requirements of FERPA and applicable state laws. Data may be disclosed for certain educational purposes and studies. Any agency or organization that is authorized by the Office of Superintendent of Public Instruction (OSPI) to access student-level data must adhere to all federal and state laws protecting student data and safeguarding the confidentiality and privacy of student records. The OSPI may collect and distribute aggregate data about students or student-level data without PII.

Current law provides that the board of directors of a school district may contract with other districts, educational service districts (ESDs), public or private organizations, agencies, schools, or individuals to implement the board's powers and duties. The board may contract for goods and services, and educational, instructional, and specialized services to improve student learning or achievement.

Parents and guardians have a right to review all education records of their students. The school boards must establish a procedures for granting parents' or guardians' requests for access to the education records of their children. These procedures must comply with FERPA.

Special Education.
Two federal laws require school districts to provide individualized education and support services to children who are eligible for special education due to a disability. The Individuals with Disabilities Education Improvement Act (commonly known as IDEA) requires that districts provide to each public school child who receives special education an Individualized Education Program (IEP). An IEP guides the delivery of special education supports and services designed to meet the child's unique needs. The Rehabilitation Act of 1973, Section 504 requires that districts provide to each qualified student with a disability regular or special education services and related services designed to meet the student's individual educational needs.

K-12 Data Governance Group.
The K-12 Data Governance Group (DGG) was established within the OSPI in 2009 to assist in the design and implementation of a K-12 education data improvement system for financial, student, and educator data. The DGG includes representatives from school districts, data users, and education agencies. The DGG defines the operating rules and governance structure for K-12 data collections, including defining and maintaining standards for privacy and confidentiality.

Summary of Bill:

Access to Student Data.
The OSPI must grant parents and legal guardians access to any student record that is a record of a child of the parent or a child in the care of the legal guardian, including records that contain personally identifiable student-level data (PID), unless the student is age eighteen or older.

School district boards of directors must include in their procedure for granting a parent or guardian's requests for access to the education records of his or her child that:
- the records must be provided electronically, if practicable;
- no fee may be charged for the inspection of records; and

- if the records are provided in a nonelectronic format, then the district may impose a reasonable charge to cover the actual costs directly incident to the copying.

Students may download, export, or otherwise save or maintain their own student data or documents.

Use and Disclosure of Student Data.
Any public agencies or organizations or any private contractors or vendors authorized by the OSPI, an ESD, or a school district board of directors to access student-level data must comply with federal and state laws related to student data privacy, security, and confidentiality. Recipients of PID from the OSPI, an ESD, or school board, to the extent they are providing services to these organizations, must ensure:

- all PID is used solely for the purpose for which the disclosure was intended;
- no PID is sold or used for secondary purposes such as marketing or targeted advertising;
- all PID, including backup copies, is destroyed when it is no longer required for the purposes for which it was disclosed, or upon agreement or contract termination, or project completion;
- a record is kept of any requests for access to the PID; and
- no PID is disclosed to any other individual or entity without the prior written consent of the parent, legal guardian, or student if the student is age eighteen or older, unless the entity is an educational agency or institution that abides by the data security requirements of this section, and FERPA and corresponding regulations.

These provisions do not apply to use or disclosure of PID by a private contractor or vendor to a service provider, provided the private contractor or vendor:

- prohibits the service provider from using any PID for any purpose other than providing the contracted service to, or on behalf of, the private contractor or vendor for the educational purposes for which such data was originally disclosed to the private contractor or vendor;
- prohibits the service provider from disclosing any PID provided by the private contractor or vendor to subsequent third parties unless the disclosure is otherwise permitted by this section; and
- requires the service provider to comply with the requirements of this section.

"PID" means any information collected by the OSPI, any state or local educational agency or institution, the board of directors of a school district, or any third-party service provider or contractor on behalf of the foregoing related to a particular identified or identifiable student in Washington, including:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number, or student number;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

PID does not include any anonymous and aggregated data that cannot be used to link specific information to a particular student. The definition of PID is substantially similar to the federal definition of PII, except that it does not include biometric information or records

Data Security.
Any public agency or organization that possesses PID must take special precautions to avoid accidental disclosure of the data, including encryption whenever feasible. Private contractors or vendors must employ industry standard methods to ensure security of all PID that they receive, store, use, and transmit.

The DGG must develop a detailed data security plan and procedures to govern the use and maintenance of data systems, including ensuring the use of appropriate administrative, physical, and technical safeguards for electronic and physical PID at the state level; and develop a model plan consistent with this act for school districts to use to safeguard PID at the school district level.

Directory Information.
The OSPI, ESDs, and school boards or schools may release directory information to make authorized school enhancement products and services available to parents and students, as long as any outside party receiving directory information for these purposes is prohibited from secondary use or sale of the information and is required to comply with student data, disclosure, and security provisions. The term "directory information" has the same meaning as it has under FERPA.

Aggregate Data.
School districts may collect and distribute aggregate data about students, or student-level data without personally identifiable information.

Personalized Learning.
PID may be used for adaptive learning, personalized learning, or customized education.

Biometric Information.
Unless necessary to implement an IEP or section 504 plan, student biometric information may not be collected, retained, or used by the following:

- the OSPI, or any employee or contractor of the OSPI;
- any ESD, or any employee or contractor of an ESD; and
- any school board, school, employee or contractor of a school district or school.

"Biometric information" has the same meaning as "biometric record," under FERPA.

Definitions.
Definitions are also provided for the terms: school enhancement products and services, and targeted advertising.

Appropriation: None.

Fiscal Note: Requested on March 10, 2015.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.