WEST VIRGINIA LEGISLATURE

2016 REGULAR SESSION

ENGROSSED

Committee Substitute

for

House Bill 4261

(BY DELEGATES SHOTT, MCCUSKEY, COWLES, O'NEAL,

BUTLER, MARCUM, SHAFFER, SOBONYA, FOLK,

OVERINGTON AND AZINGER)

[Introduced January 25, 2016;

originating in the Committee on the Judiciary.]

A BILL to amend and reenact §18-2-5h of the Code of West Virginia, 1931, as amended, relating to student data; prohibiting the department from transferring confidential student information to federal, state or local agencies or other persons or entities; providing for exceptions; authorizing student or redacted data to be provided as part of a contract with a vendor; and adding a new exception providing for the sharing of certain information in the event that the ACT or SAT tests are adopted for use as the state summative assessment.

Be it enacted by the Legislature of West Virginia:

That §18-2-5h of the Code of West Virginia, 1931, as amended, be amended and reenacted to read as follows:

ARTICLE 2. STATE BOARD OF EDUCATION.

§18-2-5h. Student Data Accessibility, Transparency and Accountability Act.

(a) *Title*. — This section shall be known and may be cited as the "Student Data Accessibility, Transparency and Account-ability Act."

(b) *Definitions.* — As used in this section, the following words have the meanings ascribed to them unless the context clearly implies a different meaning:

(1) "Board" means the West Virginia Board of Education;

(2) "Department" means the West Virginia Department of Education;

(3) "Student Data system" means the West Virginia Department of Education statewide longitudinal data system;

(4) "Aggregate data" means data collected that is reported at the group, cohort, or institutional level with a data set of sufficient size that no information for an individual parent or student is identifiable;

(5) "Redacted data" means a student dataset in which parent and student identifying information has been removed;

(6) “State-assigned student identifier” means the unique student identifier assigned by the state to each student that shall not be or include the Social Security number of a student in whole or in part;

(7) “Student data” means data collected or reported at the individual student level included in a student’s educational record;

(8) “Provisional student data” means new student data proposed for inclusion in the student data system;

(9) “School district” means a county board of education, the West Virginia Schools for the Deaf and Blind and the West Virginia Department of Education with respect to the education programs under its jurisdiction that are not in the public schools;

(10) “Directory information” means the following individual student information that is subject to disclosure for school-related purposes only: Student name, address, telephone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, indication of “graduate” or “nongraduate,” degrees and awards receives, most recent previous school attended, and photograph.

(11) “Confidential student information” means data relating to a person’s Social Security number, or other identification number issued by a state or federal agency, except for the state-assigned student identifier as defined in this section, religious affiliation, whether the person or a member of their household owns or possesses a firearm, whether the person or their family are or were recipients of financial assistance from a state or federal agency, medical, psychological or behavioral diagnoses, criminal history, criminal history of parents, siblings or any members of the person’s household, vehicle registration number, driver’s license number, biometric information, handwriting sample, credit card numbers, consumer credit history, credit score, or genetic information;

(12) “Affective computing” means human-computer interaction in which the device has the ability to detect and appropriately respond to its user’s emotions and other stimuli; and

(13) “Fair Information Practice Principles” are United States Federal Trade Commission guidelines that represent widely accepted concepts concerning fair information practice in an electronic marketplace.

(c) *Data Inventory – State Responsibilities. —* The Department of Education shall:

(1) Create, publish, and make publicly available a data inventory and dictionary or index of data elements with definitions of individual student data fields in the student data system to include, but not be limited to:

(A) Any individual student data required to be reported by state and federal education mandates;

(B) Any individual student data which has been proposed in accordance with paragraph (A), subdivision (7) of this subsection for inclusion in the student data system with a statement regarding the purpose or reason and legal authority for the proposed collection; and

(C) Any individual student data that the department collects or maintains with no current identified purpose;

(2) Develop, publish, and make publicly available policies and procedures to comply with all relevant state and federal privacy laws and policies, including, but not limited to, the Federal Family Educational Rights and Privacy Act (FERPA) and other relevant privacy laws and policies. The policies and procedures specifically shall include, but are not limited to:

(A) Access to student and redacted data in the statewide longitudinal data system shall be restricted to:

(i) The authorized staff of the department and the contractors working on behalf of the department who require access to perform their assigned duties as required by law and defined by interagency data-sharing agreements;

(ii) District administrators, teachers and school personnel who require access to perform their assigned duties;

(iii) Students and their parents; and

(iv) The authorized staff of other West Virginia state agencies as required by law and defined by interagency data-sharing agreements;

(B) Ensure that any inter-agency data-sharing agreements shall be posted on the Department website, and parents shall be notified of their right to opt out of sharing the child's data pursuant to agreements.

(C) Use only aggregate data in public reports or in response to record requests in accordance with this section;

(D) Unless otherwise prohibited by law, develop criteria for the approval of research and data requests from state and local agencies, the Legislature, researchers working on behalf of the department, and the public. Student data maintained by the department shall remain redacted; and

(E) Notification to students and parents regarding student privacy rights under federal and state law;

(3) Unless otherwise provided by law, the department shall not transfer confidential student information or redacted data that is confidential under this section to any federal, state or local agency or other ~~organization~~ person or entity, public or private, with the following exceptions:

(A) A student transfers out-of-state or a school or school district seeks help with locating an out-of-state transfer;

(B) A student leaves the state to attend an out-of-state institution of higher education or training program;

(C) A student registers for or takes a national or multistate assessment;

(D) A student voluntarily participates in a program for which a data transfer is a condition or requirement of participation;

(E) The department enters into a contract that governs databases, assessments, student or redacted data, special education or instructional supports with an in-state or out-of-state contractor for the purposes of state level reporting;

(F) A student is classified as “migrant” for federal reporting purposes; ~~or~~

(G) A federal agency is performing a compliance review; or

(H) In the event that the ACT or the SAT tests are adopted for use as the state summative assessment, nothing in this article prevents the ACT or the College Board from using a student’s assessment results and necessary directory or other permissible information under this Act. If information classified as confidential is required, the ACT, SAT or college board must obtain affirmative written consent from the student (if 18 or older) or the student’s parent or guardian and provided that the consent contain a detailed list of confidential information required and the purpose of its requirement.

(4) Develop a detailed data security plan that includes:

(A) Guidelines for the student data system and for individual student data including guidelines for authentication of authorized access;

(B) Privacy compliance standards;

(C) Privacy and security audits;

(D) Breach planning, notification and procedures;

(E) Data retention and disposition policies; and

(F) Data security policies including electronic, physical, and administrative safeguards, such as data encryption and training of employees;

(5) Ensure routine and ongoing compliance by the department with FERPA, other relevant privacy laws and policies, and the privacy and security policies and procedures developed under the authority of this act, including the performance of compliance audits;

(6) Ensure that any contracts that govern databases, assessments or instructional supports that include student or redacted data and are outsourced to private vendors include express provisions that safeguard privacy and security and include penalties for noncompliance; and

(7) Notify the Governor and the Legislature annually of the following:

(A) New student data proposed for inclusion in the state student data system. Any proposal by the Department of Education to collect new student data must include a statement regarding the purpose or reason and legal authority for the proposed collection. The proposal shall be announced to the general public for a review and comment period of at least sixty days and approved by the state board before it becomes effective. Any new student data collection approved by the state board is a provisional requirement for a period sufficient to allow schools and school districts the opportunity to meet the new requirement;

(B) Changes to existing data collections required for any reason, including changes to federal reporting requirements made by the U.S. Department of Education and a statement of the reasons the changes were necessary;

(C) An explanation of any exceptions granted by the state board in the past year regarding the release or out-of-state transfer of student or redacted data; and

(D) The results of any and all privacy compliance and security audits completed in the past year. Notifications regarding privacy compliance and security audits shall not include any information that would itself pose a security threat to the state or local student information systems or to the secure transmission of data between state and local systems by exposing vulnerabilities.

(8) Notify the Governor upon the suspicion of a data security breach or confirmed breach and upon regular intervals as the breach is being managed. The parents shall be notified as soon as possible after the suspected or confirmed breach.

(9) Prohibit the collection of confidential student information as defined in subdivision ten of subsection (b) of this section.

(d) *Data Inventory – District Responsibilities. —* A school district shall not report to the state the following individual student data:

(1) Juvenile delinquency records;

(2) Criminal records;

(3) Medical and health records; and

(4) Student biometric information.

(e) *Data Inventory – School Responsibilities.* — Schools shall not collect the following individual student data:

(1) Political affiliation and beliefs;

(2) Religion and religious beliefs and affiliations;

(3) Any data collected through affective computing;

(4) Any data concerning the sexual orientation or beliefs about sexual orientation of the student or any student's family member; and

(5) Any data concerning firearm's ownership by any member of a student's family.

(f) *Data Governance Manager.* — The state superintendent shall appoint a data governance manager, who shall report to and be under the general supervision of the state superintendent. The data governance manager shall have primary responsibility for privacy policy, including:

(1) Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of student data;

(2) Assuring that student data contained in the student data system is handled in full compliance with the Student Data Accessibility, Transparency, and Accountability Act, FERPA, and other state and federal privacy laws;

(3) Evaluating legislative and regulatory proposals involving collection, use, and disclosure of student data by the Department of Education;

(4) Conducting a privacy impact assessment on proposed rules of the state board and department in general and on the privacy of student data, including the type of personal information collected and the number of students affected;

(5) Coordinating with the general counsel of the state board and department, other legal entities, and organization officers to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner;

(6) Preparing a report to the Legislature on an annual basis on activities of the department that affect privacy, including complaints of privacy violations, internal controls, and other matters;

(7) Establishing department-wide policies necessary for implementing Fair Information Practice Principles to enhance privacy protections;

(8) Working with the Office of Data Management and Analysis, the general counsel, and other officials in engaging with stakeholders about the quality, usefulness, openness, and privacy of data;

(9) Establishing and operating a department-wide Privacy Incident Response Program to ensure that incidents are properly reported, investigated and mitigated, as appropriate;

(10) Establishing and operating a process for parents to file complaints of privacy violations;

(11) Establishing and operating a process to collect and respond to complaints of privacy violations and provides redress, as appropriate; and

(12) Providing training, education and outreach to build a culture of privacy across the department and transparency to the public.

The data governance manager shall have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the department that relate to programs and operations with respect to his or her responsibilities under this section and shall make investigations and reports relating to the administration of the programs and operations of the department as are necessary or desirable.

(g) *Parental rights regarding child's information and education record.* —Parents have the right to inspect and review their child's education record maintained by the school and to request student data specific to their child's educational record. School districts must provide parents or guardians with a copy of their child's educational record upon request. Whenever possible, an electronic copy of the educational record must be provided if requested and the identity of the person requesting the information is verified as the parent or guardian.

The state board shall develop guidance for school district policies that:

(1) Annually notify parents of their right to request student information;

(2) Ensure security when providing student data to parents;

(3) Ensure student data is provided only to the authorized individuals;

(4) Detail the timeframe within which record requests must be provided;

(5) Ensure that school districts have a plan to allow parents to view and access data specific to their child's educational record and that any electronic access provided is restricted to eligible parties;

(6) Ensure compliance in the collection, use and disclosure of directory information and providing parents or guardians with a form to limit the information concerning their child in directory and subject to release; and

(7) Informing parents of their rights and the process for filing complaints of privacy violations.

(h) *State Board Rules.* — The state board shall adopt rules necessary to implement the provisions of the Student Data Accessibility, Transparency, and Accountability Act.

(i) *Effect on Existing Data.* — Upon the effective date of this section, any existing student data collected by the Department of Education shall not be considered a new student data collection under this section.

NOTE: Strike-throughs indicate language that would be stricken from a heading or the present law and underscoring indicates new language that would be added.