State of Arkansas *As Engrossed: S2/10/15 S3/10/15*
90th General Assembly
Regular Session, 2015

A Bill

SENATE BILL 218

By: Senator A. Clark

For An Act To Be Entitled

AN ACT TO ESTABLISH THE STUDENT DATA ACCESSIBILITY, TRANSPARENCY, AND ACCOUNTABILITY ACT; TO PROTECT STUDENT DATA; AND FOR OTHER PURPOSES.

Subtitle

TO ESTABLISH THE STUDENT DATA ACCESSIBILITY, TRANSPARENCY, AND ACCOUNTABILITY ACT.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

SECTION 1. Arkansas Code Title 6, Chapter 18, is amended to add an additional subchapter to read as follows:

Subchapter 20 - Student Data Accessibility, Transparency, and Accountability Act.

6-18-2001. Established.

There is established the Student Data Accessibility, Transparency, and Accountability Act.

6-18-2002. Legislative intent.

(a) It is the intent of the General Assembly to ensure that:

(1) Student data is safeguarded; and

(2) The wishes of students and the parents regarding students' privacy are honored, respected, and protected.

(b) The General Assembly acknowledges that student data:

(1) Is a vital resource for parents, teachers, and school staff;

(2) Allows parents and students to make more informed choices about educational programs and better gauge a student's educational progress and needs;

(3) Is used by teachers and school staff in:

(A) Planning responsive educational programs and services for students;

(B) Scheduling students into appropriate classes; and

(C) Completing reports for educational agencies;

(4) Is critical in helping educators assist students in successfully graduating from high school and being prepared to enter the workforce or postsecondary education; and

(5) In emergency situations, should be readily available to school officials and emergency personnel to assist students and their families.

(c) The General Assembly believes that while student information is important for educational purposes, it is critically important to ensure that student information is protected, safeguarded, kept private, and only used by appropriate educational authorities to serve the best interests of the student.

6-18-2003. Definitions.

As used in this subchapter:

(1) "Aggregate data" means data that is not personally identifiable and that is collected or reported at a group, cohort, or institutional level;

(2) "Education record" means an education record as defined in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g;

(3) "Eligible student" means a student who is eighteen (18) years of age or older or is attending an institution of higher education;

(4) "Provisional student data" means new student data proposed for inclusion in the state student data system;

(5) "Redacted data" means a student data set that has been deidentified and that does not permit, alone or in combination with other deidentified data, the information to be personally identified with an individual student or student's family;

(6) "State-assigned student identifier" means the unique student identifier assigned by the state to a student that does not include the Social Security number of a student in whole or in part;

(7) "State data system" means the longitudinal data system maintained by the Department of Education.

(8) "Student data" means data collected or reported at the individual student level included in a student's educational record including without limitation:

(A) State-administered assessment results, including participation information;

(B) Courses taken, completed, credits earned, and other transcript information;

(C) Course grades and grade point averages;

(D) Grade level and expected graduation date or year;

(E) Degree, diploma, credential attainment, or other school exit information;

(F) Attendance and mobility information between and within school districts;

(G) Date of birth, full name, gender, race, and ethnicity; and

(H) Program participation information required by state or federal law; and

6-18-2004. Chief Privacy Officer.

(a)(1) The Commissioner of Education shall appoint a Chief Privacy Officer.

(2) The officer shall assume the primary responsibility for data privacy and security policy including without limitation:

(A) Assuring that the use of technologies strengthen privacy protections related to the use, collection, and disclosure of student data;

(B) Assuring that student data contained in the state data system is handled in full compliance with this subchapter, the Family Educational Rights and Privacy Act (FERPA), and other relevant state or federal laws;

(C) Evaluating legislative and regulatory proposals

involving the collection, use, or disclosure of student data by the Department of Education;

(D) Conducting a privacy impact assessment on a proposed legislative proposal, agency regulation, or program initiative of the department, including the type of personal information collected and the number of students impacted;

(E) Coordinating with the department's legal staff to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner;

(F) Preparing an annual report to the General Assembly regarding activities of the department that affect privacy, including complaints of privacy violations, internal controls, and other matters;

(G) Establishing department policies necessary for implementing Fair Information Practice Principles published by the Fair Trade Commission, as appropriate, to enhance privacy protections;

(H) Working with other officials and stakeholders concerning the quality, usefulness, openness, and privacy of data;

(I) Establishing and operating a department policy addressing data breaches and other incidents to ensure that breaches and incidents are reported, investigated, and mitigated, as appropriate;

(J) Establishing and operating a process for a parent to file a complaint concerning a privacy violation or the inability to access the education record of his or her child;

(K) Providing training, education, and outreach to build a culture of privacy and transparency to the public among all state and local governmental entities that collect, store, use, or share student data; and

(L) Developing policies and procedures for the state and school district to adopts regarding third party access, collection, storage, use, or sharing of student data.

(b) The officer may investigate issues of compliance with this subchapter and with other state or federal laws concerning student data or privacy by the department and local educational agencies and may:

(1) 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 the

responsibilities of the officer under this section; and

(2) Make investigations and reports related to the administration of this subchapter as necessary.

(c) The officer shall report to and be under the supervision of the commissioner.

6-18-2005. Data inventory — Responsibilities.

The Department of Education shall:

(1) Create, publish, and make publically available a data inventory and dictionary or index of data elements with definitions of each student data field in the student data system including without limitation, individual student data that:

(A) Is required to be reported by state or federal law, regulation, or program;

(B) Is included or has been proposed to be included in the student data system with a statement regarding the purpose or reason for the proposed collection; and

(C) Is collected or maintained by the *Department of Education* with no current identified purpose;

(2) Develop, publish, and make publicly available polices and procedures for the student data system to comply with this subchapter or other relevant state or federal laws or regulations including without limitations policies and procedures that:

(A) Restrict or grant access to student data in the student data system;

(B) Prohibit the use of data other than aggregate or redacted data in public reports;

(C) Are consistent with applicable law, criteria for the approval of research and data requests from state and local agencies, the requirements of General Assembly, and research done on behalf of the *Department of Education* and the public; and

(D) Ensure at least annual notifications to eligible students and parents *of the* students regarding student privacy rights;

(3) Unless otherwise provided by law or approved by the State Board of Education, not transfer student data to a federal, state, or local agency, or nongovernmental organization, except for disclosures incident to

the following actions:

(A) A student transfers to another public school or school district or a school district seeks help with locating a transfer student;

(B) A student enrolls in an institution of higher education or a postsecondary training program;

(C) A student registers for or takes a national or multistate assessment and the data is required to administer the assessment;

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

(E) The *Department of Education* enters into a contract that governs databases, assessments, special education, or instructional supports with a contractor for the purpose of state level reporting;

(F) The federal government requires the transfer of student data for a student classified as a "migrant" for related federal program purposes;

(G) A federal agency requires the data to perform an *audit, compliance review, or complaint investigation; or*

(H) A contractor who maintains a statewide longitudinal data system if the contractor has a valid memorandum of understanding, contract, or professional services grant with the Department of Human Services, the Department of Higher Education, or the Department of Workforce Services that permits the sharing of student data with the contractor.

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

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

(B) Privacy and security audits;

(C) Plans for responding to security breaches, including notifications and related procedures;

(D) Data retention and disposition;

(E) Data security, including electronic, physical, and administrative safeguards, such as data encryption and employee training;

(F) Standards concerning the minimum number of students or information that may be included in a data set in order for the data to be considered aggregated; and

(G) A process for continually updating the data security

plan, at minimum on an annual basis, in order to identify and address any risks to the security of student data;

(5) Ensure routine and ongoing compliance by the *Department of Education* with state and federal laws and regulations concerning student privacy, including the performance of compliance audits;

(6) Review and approve polices and procedures developed by the Chief Privacy Officer under this subchapter; and

(7) Annually notify the Governor and the General Assembly of the following matters related to the student data system:

(A)(i) New student data proposed for inclusion in the system.

(ii) Any new student data collection proposed by the *Department of Education* or the state board is a provisional requirement until the school districts have the opportunity to meet the new requirement.

(iii) The state board shall announce a proposed provisional student data requirement to the public for review and comment at least sixty (60) days before adoption;

(B) Changes to existing data collections required for any reason, including changes to federal reporting requirements;

(C) A list of any exceptions granted by the state board in the past year regarding the release or transfer of student data;

(D) The results of all privacy compliance and security audits completed in the past year; and

(E) Information regarding a request for access to student data by a student or parent, including the responsiveness of the *Department of Education* to the request.

6-18-2006. Student information and data collection — Reporting restrictions.

(a) Unless required by state or federal law, or in the case of a health or safety emergency, a school district shall not report to the state the following individual student data or student information:

(1) Juvenile delinquency records;

(2) Criminal records;

(3) Medical or health records; or

(4) Student biometric information.

(b) Unless required by state or federal law, or in the case of a health or safety emergency, a public school shall not collect the following data on a student of the student's family:

(1) Political affiliation;

(2) Voting history;

(3) Income, except as required to apply for or administer a program to assist a student from a low income family; or

(4) Religious affiliation or beliefs.

6-18-2007. Contracts with third parties.

The Department of Education, through the Chief Privacy Officer, shall ensure that a contract with a third party, including a private vendor or other nongovernmental entity, and a state agency or local educational agency, that involves the disclosure of student data or student-generated information, includes a:

(1) Statement that the education records and student data continue to be the property of and under the control of the state agency or local educational agency;

(2) Description of the means by which a student or student's parent may retain control of the student-generated content, if applicable, including options for a student to transfer student-generated content to a personal account;

(3) Prohibition against the third party using student data for any purpose other than those required or permitted by the contract;

(4) Description of the actions the third party will take to ensure the security and confidentiality of the student data;

(5) Description of the procedures for notifying the student or the student's parent in the event of an unauthorized disclosure;

(6) Certification that the student data will not be retained or available to the third party upon completion of the contract;

(7) Description of how the third party will ensure compliance with the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g;

(8) Prohibition against the third party using or permitting others to use student data to engage in targeted advertising;

(9) Prohibition against the third party collecting any of the information listed in § 6-18-2006(b); and

(10) Prohibition of any unilateral changes to the contract by the third party.

6-18-2008. Requests for information – Complaints.

(a)(1) An eligible student or the parent of a student may review the student's education record maintained by a public school or school district.

(2) An eligible student or the parent of a student may request a copy of student data that is included in the student's education record.

(b) A public school or school district shall provide an eligible student or the parent of a student with an electronic copy of the student's education record upon request.

(c) The Department of Education shall develop a policy for a school district to:

(1) Annually notify an eligible student or the parent of a student of the right to request student information;

(2) Ensure student information is kept secure when it is provided;

(3) Ensure that student information is provided only to authorized individuals;

(4) Produce student data and education record requests to eligible students or the parent of a student within three (3) business days of receiving the request; and

(5) Ensure that a public school or school district has a plan to allow an eligible student or parent of a student to view online, download, and transmit data specific to the student's educational record.

(d)(1) The Chief Privacy Officer shall develop a policy and procedure for an eligible student or the parent of a student to file a complaint with the state agency or local educational agency that has violated this act or other state or federal laws or regulations with regard to privacy.

(2) In responding to a complaint, the officer may:

(A) Investigate the allegation;

(B) Dismiss the complaint if it fails to allege any violation of this subchapter;

(C) Issue a written advisory opinion within thirty (30) calendar days after the complaint is filed concerning whether or not a violation occurred, which shall be available to the public except for those

portions of the opinion that could reveal the identity of the student; and

(D) Recommend to the Commissioner of Education or school district administrators that a breach of contract complaint or other action be taken against a third contractor, if applicable.

6-18-2009. Providing student data to the Bureau of Legislative Research.

Nothing in this subchapter prevents the Department of Education, a school district, public school or local educational agency from providing student data to the Bureau of Legislative Research.

6-18-2010. Rules.

The State Board of Education shall promulgate rules to administer this subchapter.

/s/A. Clark