SENATE BILL 1470

By Gresham

AN ACT to amend Tennessee Code Annotated, Title 10, Chapter 7, Part 5 and Title 49, relative to data.

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

SECTION 1. Tennessee Code Annotated, Title 49, Chapter 1, is amended by adding Sections 2 through 5 as a new, appropriately designated part.

SECTION 2. This part shall be known and may be cited as the "Data Accessibility, Transparency and Accountability Act".

SECTION 3. As used in this part:

(1) "Aggregate data" means data collected or reported at the group, cohort, or institutional level;

(2) "Board" or “state board” means the state board of education;

(3) "Data system" means the body of student data collected by the department of education;

(4) "De-identified data" means a student dataset in which parent and student identifying information, including the personal identification number, has been removed;

(5) "Department" means the department of education;

(6) “FERPA” means the federal Family Educational Rights and Privacy Act, codified at 20 U.S.C. § 1232g;

(7) "Personal identification number" means the unique student identifier assigned to a student under § 49-6-5101;

(8)

(A) "Student data" means data collected or reported at the individual student level that is included in a student's educational record;

(B) "Student data" includes:

(i) State and national assessment results, including information on untested public school students;

(ii) Course taking and completion, credits earned and other transcript information;

(iii) Course grades and grade point average;

(iv) Date of birth, grade level and expected graduation date or graduation cohort;

(v) Degree, diploma, credential attainment and other school exit information such as receipt of the GED® and drop-out data;

(vi) Attendance and mobility;

(vii) Data required to calculate the federal four-year adjusted cohort graduation rate, including sufficient exit and drop-out information;

(viii) Discipline reports limited to objective information sufficient to produce the federal Title IV annual incident report;

(ix) Remediation;

(x) Special education data; and

(xi) Demographic data and program participation information; and

(C) Unless included in a student's educational record, "student data" does not include:

(i) Juvenile delinquency records;

(ii) Criminal records;

(iii) Medical and health records;

(iv) Student social security number; and

(v) Student biometric information; and

(9) “Teacher data” means personal summative and evaluation scores, the access to which is limited to LEA administrators, local boards of education, or those with direct supervisory authority who require such access to perform their assigned duties.

SECTION 4. The state board 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 currently in the student data system including any individual student data that:

(A) Is required to be reported by state and federal education mandates;

(B) Has been proposed for inclusion 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 with no current purpose or reason;

(2) Develop, publish and make publicly available policies and procedures to comply with FERPA, § 10-7-504 and other relevant privacy laws and policies. These policies and procedures shall, at a minimum, require that:

(A) Access to student and de-identified data in the student data system is restricted to:

(i) The authorized staff of the department and the department's contractors who require access to perform their assigned duties;

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

(iii) Students and their parents; provided, however, that a student or the student’s parents may only access the student’s individual data; and

(iv) The authorized staff of other state agencies as required by law;

(B) The department use only aggregate data in public reports or in response to record requests in accordance with subdivision (3);

(C) The commissioner develops criteria for the approval of research and data requests from state and local agencies, the general assembly, researchers and the public; provided, however, that:

(i) Unless otherwise approved by the state board, student data maintained by the department shall remain confidential; and

(ii) Unless otherwise approved by the state board to release student or de-identified data in specific instances, the department may only use aggregate data in the release of data in response to research and data requests; and

(D) Students and parents are notified of their rights under federal and state law.

(3) Unless otherwise approved by the state board, the department shall not transfer student or de-identified data deemed confidential under subdivision (2)(C)(i) to any federal, state or local agency or other organization or entity outside of the state, except when:

(A) A student transfers out of state or an LEA 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 such a data transfer is a condition or requirement of participation;

(E) The department enters into a contract that governs databases, assessments, special education or instructional supports with an out-of-state vendor; or

(F) A student is classified as "migrant" for federal reporting purposes;

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

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

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

(C) Privacy compliance standards;

(D) Privacy and security audits;

(E) Breach planning, notification and procedures; and

(E) Data retention and disposition policies;

(5) Ensure routine and ongoing compliance by the department with FERPA, § 10-7-504, other relevant privacy laws and policies, and the privacy and security policies and procedures developed under the authority of this part, including the performance of compliance audits;

(6) Ensure that any contracts that govern databases, assessments or instructional supports that include student or de-identified 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 general assembly annually of the following:

(A) New student data proposed for inclusion in the state student data system; provided, however, that:

(i) Any new student data collection proposed by the state board shall become a provisional requirement to allow LEAs and their local data system vendors the opportunity to meet the new requirement; and

(ii) In order to make any new provisional student data collection a permanent requirement, the state board shall submit the provisional student data collection to the governor and the education committees of the senate and the house of representatives for their review and recommendations within one (1) year. Any provisional student data collection not approved by resolutions of the senate and house of representatives before the next general assembly is chosen shall expire and no longer be required;

(B) Changes to existing data collections required for any reason, including changes to federal reporting requirements made by the United States department of education;

(C) Any exceptions granted by the state board in the past year regarding the release or out-of-state transfer of student or de-identified data accompanied by an explanation of each exception; 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.

SECTION 5.

(a) The commissioner of education shall designate an employee of the department as the chief privacy officer. The chief privacy officer shall be under the general supervision of the commissioner.

(b) The chief policy officer shall:

(1) Report directly to the commissioner; and

(2) Assume primary responsibility for privacy policy, including:

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

(B) Assuring that student data contained in the department's student data system is handled in full compliance with this act, FERPA, § 10-7-504 and other state and federal privacy laws;

(C) Evaluating legislative and regulatory proposals involving collection, use, and disclosure of student data by the department;

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

(E) Coordinating with the office of the general counsel, 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;

(F) Preparing a report to the general assembly on an annual basis on activities of the department that affect privacy, including complaints of privacy violations, internal controls and other manners;

(G) Establishing department-wide policies necessary for implementing fair information practice principles to enhance privacy protections;

(H) Working with the general counsel and other departmental employees and state officials in engaging with stakeholders about the quality, usefulness, openness and privacy of data;

(I) Establishing and operating a department-wide privacy incident response program to ensure that incidents are properly reported, investigated and mitigated, as appropriate;

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

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

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

(c) The commissioner may authorize the chief privacy officer to investigate a violation of the privacy policy. In conducting an investigation, the chief privacy officer 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 chief privacy officer under this section; and

(2) Make such investigations and reports relating to the administration of the programs and operations of the department as are necessary or desirable.

SECTION 6.

(a) Parents and guardians have the right to inspect and review their children's education records maintained by the school.

(b) Parents and guardians have the right to request student data specific to their children's educational records.

(c) LEAs shall provide parents or guardians with an electronic copy of their children's educational records upon request.

(d)

(1) The department shall develop a model student records policy for LEAs that requires an LEA to:

(A) Annually notify parents and guardians of their right to request student information;

(B) Ensure security when providing student data to parents or guardians;

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

(D) Set the timeframe within which record requests must be provided; and

(E) Ensure that LEAs have a plan to allow parents and guardians to view online, download, and transmit data specific to their children's educational records.

(2) The department shall develop the model student records policy by December 31, 2014. An LEA shall adopt the model policy or develop its own policy prior to the beginning of school for the 2015-2016 school year. Before implementing a policy other than the model policy, an LEA shall submit the policy to the department for approval.

SECTION 7. LEAs and schools shall not collect individual student data on:

(1) Political affiliation; and

(2) Religion.

SECTION 8. Any collection of student data by the department existing on July 1, 2014, shall not be considered a new student data collection in accordance with subdivision (7)(A) of Section 4 of this act.

SECTION 9. The state board is authorized to promulgate rules and regulations to effectuate the purposes of this act. All such rules and regulations shall be promulgated in accordance with Tennessee Code Annotated, Title 4, Chapter 5.

SECTION 10. This act shall take effect July 1, 2014, the public welfare requiring it.