

Regular Session, 2014

SENATE BILL NO. 449

BY SENATORS APPEL AND LAFLEUR

STUDENTS. Provides relative to the privacy and protection of student data for students enrolled in public elementary, secondary, and postsecondary educational institutions. (gov sig)

1 AN ACT

2 To enact Chapter 45 of Title 17 of the Louisiana Revised Statutes of 1950, to be comprised
3 of R.S. 17:4051 through 4055, relative to student data; to require the State Board of
4 Elementary and Secondary Education and the postsecondary education management
5 boards to develop and implement policies and procedures to ensure the privacy and
6 protection of student data; to provide for definitions and policy requirements; to
7 provide relative to the appointment of chief privacy officers and their duties; to
8 provide relative to implementation; to provide for rules; and to provide for related
9 matters.

10 Be it enacted by the Legislature of Louisiana:

11 Section 1. Chapter 45 of Title 17 of the Louisiana Revised Statutes of 1950,
12 comprised of R.S. 17:4051 through 4055, is hereby enacted to read as follows:

13 **CHAPTER 45. PRIVACY AND PROTECTION OF STUDENT DATA**

14 **§4051. Short title**

15 **This Chapter shall be known and may be cited as the "Student Data**
16 **Privacy and Protection Act"**.

17 **§4052. Definitions**

1 As used in this Chapter, unless otherwise clearly indicated, the following

2 terms mean:

3 (1) "State board" means the State Board of Elementary and Secondary
4 Education.

5 (2) "State department" means the state Department of Education.

6 (3) "Postsecondary management board" means the Board of
7 Supervisors of Louisiana State University and Agricultural and Mechanical
8 College, the Board of Supervisors of Southern University and Agricultural and
9 Mechanical College, the Board of Supervisors for the University of Louisiana
10 System, and the Board of Supervisors of Louisiana Community and Technical
11 Colleges.

12 (4) "Data system" means any data system, including a longitudinal data
13 system, created and maintained by or through the state board, the governing
14 authority of a public elementary and secondary school, or a postsecondary
15 education management board that contains student data.

16 (5) "Aggregate data" means data collected or reported at the group,
17 cohort, or institutional level.

18 (6) "De-identified data" means a student dataset in which parent and
19 student identifying information has been removed.

20 (7) "Student identifier" means the unique student identifier assigned by
21 the state or an educational institution to each student that shall not be or
22 include the Social Security number of a student in whole or in part.

23 (8) "Student data" means data collected or reported at the individual
24 student level and included in a student's educational record.

25 (a) Student data includes:

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

28 (ii) Course taking and completion, credits earned, and other transcript
29 information.

1 (iii) Course grades and grade point average.

2 (iv) Date of birth, grade level, and expected graduation date or
3 graduation cohort.

4 (v) Degree, diploma, credential attainment, and other school exit
5 information such as General Educational Development and drop-out data.

6 (vi) Attendance and mobility.

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

9 (viii) Remediation.

10 (ix) Special education data.

11 (x) Demographic data and program participation information.

12 (b) Unless included in a student's educational record, student data shall
13 not include:

14 (i) Juvenile delinquency records.

15 (ii) Criminal records.

16 (iii) Medical and health records.

17 (iv) Student Social Security number.

18 (v) Student biometric information.

19 (9) "Provisional student data" means new student data proposed for
20 inclusion in a student data system.

21 **§4053. Student information and data; privacy; protection; policies**

22 **A. The State Board of Elementary and Secondary Education and each**
23 **postsecondary management board shall develop and oversee implementation of**
24 **a comprehensive policy which provides administrative, technical, and physical**
25 **safeguards to ensure the privacy and protection of student data.**

26 **B. The state board and each management board shall create, publish,**
27 **and make publicly available a data inventory and dictionary or index of data**
28 **elements with definitions of individual student data fields currently in the**
29 **student data system which includes:**

1 **(1) Any individual student data required to be reported by state and**
2 **federal education mandates.**

3 **(2) Any individual student data which has been proposed for inclusion**
4 **in a student data system with a statement regarding the purpose or reason for**
5 **the proposed collection.**

6 **(3) Any individual student data that the state board, the state**
7 **department, a postsecondary management board, a public school governing**
8 **authority, or any public educational institution collects or maintains with no**
9 **current purpose or reason.**

10 **C. The state board and each postsecondary management board shall**
11 **develop, publish, and make publicly available policies and procedures to comply**
12 **with the Federal Family Educational Rights and Privacy Act and any other**
13 **applicable state and federal laws and policies, including but not limited to:**

14 **(1) Access to student and de-identified data in the student data system**
15 **shall be restricted to:**

16 **(a) Authorized staff of the state board, the state department, a**
17 **postsecondary management board, the governing authority of a public**
18 **elementary and secondary school, or a public postsecondary educational**
19 **institution, and third-party private contractors working on behalf of these**
20 **entities who require such access to perform their assigned duties.**

21 **(b) School administrators, teachers, and school personnel who require**
22 **such access to perform their assigned duties.**

23 **(c) Students and their parents.**

24 **(d) Authorized staff of other state agencies as required by law or defined**
25 **by interagency data-sharing agreements or memorandums of understanding.**

26 **(2) Only aggregate data shall be used in public reports or in response to**
27 **record requests.**

28 **(3) The state board and each postsecondary management board shall**
29 **develop criteria for the approval of research and data requests from state and**

1 local agencies, the legislature, researchers, and the public.

2 (a) Unless otherwise approved by the state board or appropriate
3 postsecondary management board, student data maintained by these boards
4 and institutions under their supervision shall remain confidential.

5 (b) Unless otherwise approved by the state board or appropriate
6 postsecondary management board, only aggregate data may be used in the
7 release of data in response to research and data requests.

8 (4) Notification to students and parents regarding their rights under
9 federal and state law.

10 D. Unless otherwise approved by the state board, the state department,
11 or the appropriate postsecondary management board, student or de-identified
12 data deemed confidential pursuant to this Chapter shall not be transferred to
13 any federal, state, or local agency or other entity outside of this state, with the
14 following exceptions:

15 (1) A student transfers out-of-state or a school or district seeks help with
16 locating an out-of-state transfer.

17 (2) A student leaves the state to attend an out-of-state institution of
18 higher education or training program.

19 (3) A student registers for or takes a national or multistate assessment.

20 (4) A student voluntarily participates in a program for which such a
21 data transfer is a condition or requirement of participation.

22 (5) The state board, the state department, a postsecondary management
23 board, public school governing authority, or educational institution enters into
24 a contract that governs databases, assessments, special education, or
25 instructional supports with a private provider or vendor.

26 (6) A student is classified as "migrant" for federal reporting purposes.

27 E. The state board and each postsecondary education management
28 board shall have a detailed data security plan that includes:

29 (1) Guidelines for authorizing access to the student data system and to

1 **individual student data including guidelines for authentication of authorized**
2 **access.**

3 **(2) Privacy compliance standards.**

4 **(3) Privacy and security audits.**

5 **(4) Breach planning, notification, and remediation procedures.**

6 **(5) Data storage, retention, and disposition policies.**

7 **F. The state board and each postsecondary management board shall:**

8 **(1) Ensure routine and ongoing compliance with the Federal Family**
9 **Educational Rights Privacy Act, other relevant state and federal privacy laws**
10 **and policies, and the privacy and security policies and procedures developed**
11 **under the authority of this Chapter, including the performance of compliance**
12 **audits.**

13 **(2) Ensure that any contracts with private vendors or providers that**
14 **govern databases, assessments, or instructional supports that include student**
15 **data or de-identified data include express provisions that safeguard privacy and**
16 **security and include penalties for noncompliance.**

17 **G. The state board and each postsecondary management board shall**
18 **annually notify the legislature of the following:**

19 **(1) New student data proposed for inclusion in the state student data**
20 **system:**

21 **(a) Any new student data collection proposed by the state board, the**
22 **state department, or a postsecondary management board becomes a provisional**
23 **requirement to allow institutions and data system vendors the opportunity to**
24 **meet the new requirement.**

25 **(b) Any new "provisional" student data collection shall be submitted to**
26 **the legislature for its approval within one year in order to make the new student**
27 **data a permanent requirement. Any provisional student data collection not**
28 **approved by the legislature by the end of the next legislative session expires, is**
29 **no longer required, and shall not be collected.**

1 **(2) Changes to existing data collections required for any reason,**
2 **including changes to federal reporting requirements made by the U.S.**
3 **Department of Education.**

4 **(3) An explanation of any exceptions granted by the state board, the state**
5 **department, a postsecondary management board, or any educational institution**
6 **in the past year regarding the release or out-of-state transfer of student or**
7 **de-identified data.**

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

13 **H.(1) The state board and each postsecondary management board shall**
14 **designate a chief privacy officer who shall be responsible for ensuring that all**
15 **student data policies and procedures are followed and every precaution is taken**
16 **to ensure the privacy and protection of student data.**

17 **(2) Each chief privacy officer shall:**

18 **(a) Continually monitor emerging and evolving technology and**
19 **recommend policy changes needed to ensure the continued privacy and**
20 **protection of student data.**

21 **(b) Ensure that student data contained in a student data system is**
22 **handled in full compliance with the provisions of this Chapter and all other**
23 **applicable state and federal laws, including the Federal Family Educational**
24 **Rights Privacy Act.**

25 **I. Any data being collected and included in a data system on the effective**
26 **date of this Chapter shall not be considered new data for purposes of Subsection**
27 **(G) of this Section.**

28 **§4054. Implementation**

29 **The State Board of Elementary and Secondary Education and the**

1 postsecondary education management boards shall provide for the
2 implementation of this Chapter not later than January 1, 2015.

3 §4055. Rules

4 The state board and each postsecondary management board shall
5 promulgate rules and regulations to implement the provisions of this Chapter
6 in accordance with the Administrative Procedure Act.

7 Section 2. This Act shall become effective upon signature by the governor or, if not
8 signed by the governor, upon expiration of the time for bills to become law without signature
9 by the governor, as provided by Article III, Section 18 of the Constitution of Louisiana. If
10 vetoed by the governor and subsequently approved by the legislature, this Act shall become
11 effective on the day following such approval.

The original instrument and the following digest, which constitutes no part
of the legislative instrument, were prepared by Jeanne C. Johnston.

DIGEST

Appel (SB 449)

Proposed law provides for the "Student Data Privacy and Protection Act".

Proposed law provides for the following definitions:

- (1) "State board" means the State Board of Elementary and Secondary Education.
- (2) "State department" means the state Department of Education.
- (3) "Postsecondary management board" means the LSU Board of Supervisors, the SU Board of Supervisors, the Board of Supervisors for the UL System, and the Board of Supervisors of Louisiana Community and Technical Colleges (LCTCS).
- (4) "Data system" means any data system, including a longitudinal data system, created and maintained by or through the BESE, the governing authority of a public elementary and secondary school, or a postsecondary education management board that contains student data.
- (5) "Aggregate data" means data collected or reported at the group, cohort, or institutional level.
- (6) "De-identified data" means a student dataset in which parent and student identifying information has been removed.
- (7) "Student identifier" means the unique student identifier assigned by the state or an educational institution to each student that shall not be or include the Social Security number of a student in whole or in part.
- (8) "Student data" means data collected or reported at the individual student level and included in a student's educational record. Provides that student data includes state

and national assessment results; course taking and completion, credits earned, and other transcript information; course grades and grade point average; date of birth, grade level, and expected graduation date or graduation cohort; degree, diploma, credential attainment, and other school exit information; attendance and mobility; data required to calculate the federal four-year adjusted cohort graduation rate; remediation; special education data; and demographic data and program participation information. Provides that student data does not include, unless included in a student's educational record, juvenile delinquency records; criminal records; medical and health records; student Social Security number; or student biometric information.

- (9) "Provisional student data" means new student data proposed for inclusion in a student data system.

Proposed law requires BESE and each postsecondary management board to develop and oversee implementation of a comprehensive policy which provides administrative, technical, and physical safeguards to ensure the privacy and protection of student data. Further requires each of these boards to 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 that includes any individual student data required to be reported by state and federal education mandates, any individual student data proposed for inclusion in a student data system with a statement regarding the purpose or reason for the proposed collection, and any individual student data that the state board, the state department, a postsecondary management board, a public school governing authority, or any public educational institution collects or maintains with no current purpose or reason.

Proposed law requires BESE and the postsecondary management boards to develop, publish, and make publicly available policies and procedures to comply with the Federal Family Educational Rights and Privacy Act (FERPA) and any other applicable state and federal laws and policies. Further provides that such policies provide as follows:

- (1) Access to student and de-identified data in the student data system shall be restricted to: (a) authorized staff of the state board, the state department, a postsecondary management board, the governing authority of a public elementary and secondary school, or a public postsecondary educational institution, and third-party private contractors working on behalf of these entities who require such access to perform their assigned duties; (b) school administrators, teachers, and school personnel who require such access to perform their assigned duties; (c) students and their parents; and (d) authorized staff of other state agencies as required by law or defined by interagency data-sharing agreements or memorandums of understanding.
- (2) Only aggregate data shall be used in public reports or in response to record requests.
- (3) Requires the state board and each postsecondary management board to develop criteria for the approval of research and data requests from state and local agencies, the legislature, researchers, and the public. Provides that unless otherwise approved by the state board or appropriate postsecondary management board, student data maintained by these boards and institutions under their supervision shall remain confidential. Further provides that unless otherwise approved by the state board or appropriate postsecondary management board, only aggregate data may be used in the release of data in response to research and data requests.
- (4) Notification to students and parents regarding their rights under federal and state law.

Proposed law provides that unless otherwise approved by the state board, the state department, or the appropriate postsecondary management board, student or de-identified data deemed confidential pursuant to proposed law shall not be transferred to any federal, state or local agency or other entity outside of this state and provides for the following exceptions:

- (1) A student transfers out-of-state or a school or district seeks help with locating an out-of-state transfer.
- (2) A student leaves the state to attend an out-of-state institution of higher education or training program.
- (3) A student registers for or takes a national or multistate assessment.
- (4) A student voluntarily participates in a program for which such a data transfer is a condition or requirement of participation.
- (5) The state board, the state department, a postsecondary management board, public school governing authority, or educational institution enters into a contract that governs databases, assessments, special education, or instructional supports with a private provider or vendor.
- (6) A student is classified as "migrant" for federal reporting purposes.

Proposed law requires the state board and each postsecondary education management board to have a detailed data security plan that includes:

- (1) Guidelines for authorizing access to the student data system and to individual student data including guidelines for authentication of authorized access.
- (2) Privacy compliance standards.
- (3) Privacy and security audits.
- (4) Breach planning, notification, and remediation procedures.
- (5) Data storage, retention, and disposition policies.

Proposed law requires the state board and each postsecondary management board to:

- (1) Ensure routine and ongoing compliance with FERPA, other relevant state and federal privacy laws and policies, and the privacy and security policies and procedures developed under the authority of proposed law, including the performance of compliance audits.
- (2) Ensure that any contracts with private vendors or providers that govern databases, assessments or instructional supports that include student data or de-identified data include express provisions that safeguard privacy and security and include penalties for noncompliance.

Proposed law requires the state board and each postsecondary management board to annually notify the legislature of the following:

- (1) New student data proposed for inclusion in the state student data system: provides that any new student data collection proposed by the state board, the state department, or a postsecondary management board becomes a provisional requirement to allow institutions and data system vendors the opportunity to meet the new requirement; provides that any new "provisional" student data collection must be submitted to the legislature for its approval within one year in order to make the new student data a permanent requirement; further provides that any provisional student data collection not approved by the legislature by the end of the next legislative session expires, is no longer required, and shall not be collected.
- (2) Changes to existing data collections required for any reason, including changes to

federal reporting requirements made by the U.S. Department of Education.

- (3) An explanation of any exceptions granted by the state board, the state department, a postsecondary management board, or any educational institution in the past year regarding the release or out-of-state transfer of student or de-identified data.
- (4) The results of any and all privacy compliance and security audits completed in the past year. Further provides that notifications regarding privacy compliance and security audits shall not include any information that would itself pose a security threat to state or local student information systems or to the secure transmission of data between state and local systems by exposing vulnerabilities.

Proposed law requires the state board and each postsecondary management board to designate a chief privacy officer who shall be responsible for ensuring that all student data policies and procedures are followed and every precaution is taken to ensure the privacy and protection of student data. Provides that each chief privacy officer shall:

- (1) Continually monitor emerging and evolving technology and recommend policy changes needed to ensure the continued privacy and protection of student data.
- (2) Ensure that student data contained in a student data system is handled in full compliance with the provisions of proposed law and all other applicable state and federal law, including FERPA.

Proposed law provides that any data being collected and included in a data system on the effective date of proposed law shall not be considered new data for purposes of proposed law.

Proposed law requires BESE and postsecondary management boards to provide for the implementation of proposed law not later than January 1, 2015.

Proposed law requires BESE and each postsecondary management board to promulgate rules and regulations to implement proposed law in accordance with the Administrative Procedure Act.

Effective upon signature of the governor or lapse of time for gubernatorial action.

(Adds R.S. 17:4051 - 4055)