THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 565

Session of
2023

INTRODUCED BY PHILLIPS-HILL, MARTIN, J. WARD AND LAUGHLIN,
MARCH 28, 2023

REFERRED TO EDUCATION, MARCH 28, 2023

AN ACT

1 Amending Title 24 (Education) of the Pennsylvania Consolidated
2   Statutes, in preliminary provisions, providing for student
3   data privacy and protection; imposing duties on the
4   Department of Education; and providing for penalties.

5   The General Assembly of the Commonwealth of Pennsylvania

6 hereby enacts as follows:

7   Section 1. Part I of Title 24 of the Pennsylvania

8 Consolidated Statutes is amended by adding a chapter to read:

9   CHAPTER 5

10   STUDENT DATA PRIVACY AND PROTECTION

11 Subchapter

12   A. General Provisions

13   B. Powers and Duties

14   C. Disclosure and Use of Information

15   D. Enforcement

16   SUBCHAPTER A

17   GENERAL PROVISIONS

18 Sec.

19 501. Scope of chapter.

5 § 501. Scope of chapter.

6   This chapter relates to student data privacy and protection.

7 § 502. Legislative intent.

8   It is the intent of the General Assembly to ensure the

9 following:

10   (1) Only essential student data shall be collected.

11   (2) Student data shall be safeguarded.

12   (3) The privacy rights of students and their parents or

13 legal guardians shall be honored, respected and protected.

14 § 503. Findings and declarations.

15   The General Assembly finds and declares as follows:

16   (1) Educational entities in this Commonwealth are

17 custodians of vast amounts of personally identifiable

18 information through their collection and maintenance of

19 student data.

20   (2) It is critically important to ensure that only

21 essential student data shall be collected and that personal

22 information shall be protected, safeguarded, kept private and

23 only accessed or used by appropriate authorized persons.

24   (3) The Commonwealth lacks a sufficient plan to ensure

25 adequate protection of student data.

26   (4) The Commonwealth lacks guarantees for the protection

27 of student data and the personally identifiable information

28 contained within that data.

29   (5) Given the vast personally identifiable student

30 information held, educational entities are prime targets for

1   data and information poaching by identity thieves and other

2   hackers.

3   (6) In emergencies, certain information should be

4   readily available to school officials and emergency personnel

5   to assist students and their families.

6 § 504. Definitions.

7   The following words and phrases when used in this chapter

8 shall have the meanings given to them in this section unless the

9 context clearly indicates otherwise:

10   "Aggregate student data." Student data collected by an

11 educational entity which:

12   (1) is totaled and reported at the group, cohort,

13   school, school district, region or State level as determined

14   by the educational entity;

15   (2) does not reveal personally identifiable student

16   data; and

17   (3) cannot reasonably be used to identify, contact,

18   single out or infer information about a student or device

19   used by a student.

20   "Biometric identifier." A measurable biological or

21 behavioral characteristic that can be used for automated

22 recognition of an individual. The following apply:

23   (1) The term includes any of the following:

24   (i) A retina or iris scan.

25   (ii) A fingerprint.

26   (iii) A human biological sample.

27   (iv) A scan of the hand.

28   (v) A voice print.

29   (vi) Facial geometry.

30   (2) The term does not include any of the following:

(i) A physical description, including, but not

limited to, height, weight, hair color or eye color.

(ii) A writing sample.

(iii) A written signature.

(iv) Demographic data.

"Data authorization." A written authorization by a student

or a student's parent or legal guardian if the student is under

18 years of age to collect or share the student's student data.

"Educational entity." An organized education provider,

including, but not limited to, any of the following:

(1) A school district of any class.

(2) A board of school directors of a school district of

any class.

(3) A public school.

(4) An institution of higher education.

"Educational record." Student data or other student

information created and maintained by an educational entity or a

third party.

"Eligible student." A student who is:

(1) 18 years of age or older or an emancipated

individual; and

(2) attending an institution of higher education.

"Institution of higher education." Any of the following:

(1) A community college operating under Article XIX-A of

the act of March 10, 1949 (P.L.30, No.14), known as the

Public School Code of 1949.

(2) A State-owned institution.

(3) A State-related institution.

(4) Any other institution that is designated as State-

related by the Commonwealth.

1   (5) An accredited private or independent college or

2 university.

3   (6) A private licensed school as defined in the act of

4 December 15, 1986 (P.L.1585, No.174), known as the Private

5 Licensed Schools Act.

6 "Necessary student data." Student data required by Federal

7 or State law to conduct the regular activities of an educational

8 entity.

9 "Personally identifiable student data." Student data that,

10 by itself or in connection with other information, would enable

11 a specific student or other individual to be reasonably

12 identified.

13 "Public school." A school operated by a school district of

14 any class, intermediate unit, charter school, cyber charter

15 school or an area career and technical school.

16 "State-owned institution." An institution which is part of

17 the State System of Higher Education under Article XX-A of the

18 Public School Code of 1949 and all branches and campuses of a

19 State-owned institution.

20 "State-related institution." The Pennsylvania State

21 University, including the Pennsylvania College of Technology,

22 the University of Pittsburgh, Temple University and Lincoln

23 University and their branch campuses.

24 "Student." An individual who attends a public school or

25 institution of higher education, whether enrolled on a full-

26 time, part-time, credit or noncredit basis.

27 "Student data." Information regarding a student that is

28 descriptive of the student and collected and maintained at the

29 individual student level, regardless of physical, electronic or

30 other media or format, including, but not limited to, any of the

following:

    (1) The following information regarding the student:

        (i) Name.

        (ii) Date and location of birth.

        (iii) Social Security number.

        (iv) Gender.

        (v) Race.

        (vi) Ethnicity.

        (vii) Tribal affiliation.

        (viii) Sexual identity or orientation.

        (ix) Migrant status.

        (x) English language learner status.

        (xi) Disability status.

        (xii) Mother's maiden name.

        (xiii) Contact information, including telephone
numbers, email addresses, physical addresses and other
distinct contact identifiers.

        (xiv) Special education records or an applicable
mandate under 20 U.S.C. Ch. 33 (relating to education of
individuals with disabilities).

        (xv) An individualized education program or other
written education plan, including special education
evaluation data for the program or plan.

        (xvi) The student's identification number.

        (xvii) Local or State assessment results or the
reason for an exception from taking a local or State
assessment.

        (xviii) Courses taken and completed, credits earned
or other transcript information.

        (xix) Course grades, grade point average or another

1   indicator of academic achievement.

2   (xx) Grade level and expected graduation date.

3   (xxi) Cohort graduation rate or related information.

4   (xxii) Degree, diploma, credential attainment or

5   other school exit information.

6   (xxiii) Attendance and mobility.

7   (xxiv) Dropout data.

8   (xxv) An immunization record or the reason for an

9   exception from receiving an immunization.

10   (xxvi) Remediation efforts.

11   (xxvii) Cumulative disciplinary records.

12   (xxviii) Juvenile delinquency or dependency records.

13   (xxix) Criminal records.

14   (xxx) Medical or health records created or

15   maintained by an educational entity.

16   (xxxi) Political affiliation, voter registration

17   information or voting history.

18   (xxxii) Income or other socioeconomic information,

19   except as required by law or if an educational entity

20   determines income information is required to apply for,

21   administer, research or evaluate programs to assist

22   students from low-income families.

23   (xxxiii) Religious information or beliefs.

24   (xxxiv) A biometric identifier or other biometric

25   information.

26   (xxxv) Food purchases.

27   (xxxvi) Geolocation data.

28   (xxxvii) Any other information that either on its

29   own or collectively could reasonably be used to identify

30   a specific student.

1   (2) The following information regarding family members,

2 including parents and legal guardians, of the student:

3   (i) Name of family members.

4   (ii) Contact information for family members,

5 including telephone numbers, email addresses, physical

6 addresses and other distinct contact identifiers.

7   (iii) Education status, an educational record or

8 student data of a family member who is a student.

9 "Targeted marketing." Advertising to a student or a

10 student's parent or guardian that is selected based on

11 information obtained or inferred from the student's online or

12 offline behavior, usage of applications or student data. The

13 term does not include advertising to a student at an online

14 location based on the student's current visit to that location

15 or single search query without collection and retention of the

16 student's online activities over time. The term does not include

17 using the student's personally identifiable student data to

18 identify for the student institutions of higher education or

19 scholarship providers that are seeking students who meet

20 specific criteria, provided a written data authorization by the

21 student, or the student's parent or legal guardian if the

22 student is under 18 years of age, permits the disclosure and

23 use.

24 "Third party." A person that enters into a contract with an

25 educational entity to provide a good or service. The term

26 includes a subsequent subcontractor that may accompany the

27 person in the provision of the good or service.

28 § 505. Effect of chapter.

29 Nothing in this chapter shall be construed to prohibit or

30 otherwise limit the ability of an educational entity from

1 reporting or making available aggregate student data or other

2 collective data for reasonable usage.

3 SUBCHAPTER B

4 POWERS AND DUTIES

5 Sec.

11 § 511. Chief data privacy officer.

12 (a) Designation.--The Secretary of Education shall designate

13 an individual to serve as the chief data privacy officer within

14 the department to assume primary responsibility for student data

15 privacy and security policy.

16 (b) Specific duties.--The chief data privacy officer within

17 the department shall:

18 (1) Ensure that student data contained in the State data

19 system shall be handled in full compliance with:

20 (i) this chapter;

21 (ii) 20 U.S.C. § 1232g (relating to family

22 educational and privacy rights) and its associated

23 regulations; and

24 (iii) other Federal and State data privacy and

25 security laws.

26 (2) Establish, publish and make easily available

27 policies necessary to assure that the use of technologies

28 sustain, enhance and do not erode privacy protections

29 relating to the use, collection and disclosure of student

30 data.

(3)   Develop and provide to educational entities a model student data privacy and security plan.

(4)   Evaluate legislative and regulatory proposals involving use, collection and disclosure of student data by educational entities.

(5)   Conduct a privacy impact assessment on legislative proposals and regulations and program initiatives of the department, including the type of personal information collected and the number of students affected.

(6)   Prepare an annual report for submission to the General Assembly on activities of the department that affect privacy, including complaints of privacy violations, internal controls and other related matters.

(7)   Consult and coordinate with other representatives of the department and the Commonwealth and other persons regarding the quality, usefulness, openness and privacy of data and the implementation of this chapter.

(8)   Establish and operate a privacy incident response program to ensure that each data-related incident involving the department is properly reported, investigated and mitigated.

(9)   Establish a model process and policy for an eligible student and a student's parent or legal guardian if the student is under 18 years of age to file a complaint regarding a violation of data privacy or an inability to access, review or correct the student's student data or other information contained in the student's educational record.

(10) Provide training, guidance, technical assistance and outreach to build a culture of data privacy protection and data security among educational entities and third

1   parties.

2   (c) Investigations.--The chief data privacy officer may

3   investigate issues of compliance with this chapter or another

4   data privacy or security law concerning a matter related to this

5   chapter. In conducting the investigation, the chief data privacy

6   officer shall:

7   (1) have access to all records, reports, audits,

8   reviews, documents, papers, recommendations and other

9   materials available to the educational entity or third party

10 under investigation;

11   (2) limit the investigation and any accompanying report

12 to those matters which are necessary or desirable to the

13 effective administration of this chapter; and

14   (3) in matters related to compliance with Federal law,

15 refer the matter to the appropriate Federal agency and

16 cooperate with any investigation by the Federal agency.

17 § 512. Data inventory and data elements.

18   The department shall create and post on its publicly

19 accessible Internet website a data inventory and dictionary of

20 data elements with definitions of individual student data fields

21 currently in the student data system, including information

22 which:

23   (1) is required to be reported by Federal or State

24 education mandates;

25   (2) has been proposed for inclusion in the student data

26 system with a statement regarding the purpose or reason for

27 the proposed collection; and

28   (3) the department collects or maintains with no current

29 purpose or reason.

30 § 513. Forms.

1   The department shall develop forms, including, but not

2   limited to, the following:

3   (1) The notice of disclosure and acknowledgment under

4   section 522 (relating to notice of disclosure).

5   (2) The written data authorization to permit the

6   disclosure of information.

7   § 514. Rules and regulations.

8   The department shall promulgate rules and regulations

9   necessary to implement the provisions of this chapter.

10   § 515. Educational entities.

11   An educational entity shall:

12   (1) Subject to the approval of the chief data privacy

13   officer within the department and taking into account the

14   specific needs and priorities of the educational entity,

15   adopt and implement reasonable security policies and

16   procedures to protect educational records and student data in

17   accordance with this chapter to protect information from

18   unauthorized access, destruction, use, modification or

19   disclosure.

20   (2) Designate an individual to act as a student data

21   manager to fulfill the responsibilities under this section.

22   (3) Create, maintain and submit to the chief data

23   privacy officer under the department a data governance plan

24   addressing the protection of existing data and future data

25   records.

26   (4) Establish a review process for all requests for data

27   for the purpose of external research or evaluation.

28   (5) Prepare an annual report for submission to the chief

29   data privacy officer within the department. Each annual

30   report shall include:

16 § 521. Data ownership.

17   (a) Authority of student.--A student is the owner of the

18 student's student data and may download, export, transfer or

19 otherwise save or maintain any document, data or other

20 information created by the student that may be held or

21 maintained, in whole or in part, by an educational entity.

22   (b) Work or product.--Any work or intellectual product

23 created by a student, whether for academic credit or otherwise,

24 shall be the property of the student.

25 § 522. Notice of disclosure.

26   (a) Distribution.--An educational entity which collects

27 student data, regardless of whether that information is

28 developed and maintained as aggregate student data, shall

29 provide to each eligible student and each student's parent or

30 legal guardian if the student is under 18 years of age an annual

1 written notice outlining the conditions under which the

2 student's student data may be disclosed.

3   (b) Form.--The notice under this section shall be:

4   (1) prominent and provided as a stand-alone document;

5   (2) annually updated and distributed; and

6   (3) written in plain language that is easily

7 comprehended by an average individual.

8   (c) Contents.--The notice under this section shall:

9   (1) list the necessary and optional student data which

10 the educational entity collects and the rationale for the

11 collection of the data;

12   (2) state that student data collected may not be shared

13 without a written data authorization by the eligible student

14 or a student's parent or legal guardian if the student is

15 under 18 years of age;

16   (3) list each third party with access or control of

17 student data under a contractual agreement;

18   (4) outline the rights and responsibilities under this

19 chapter; and

20   (5) contain an acknowledgment specifying that the

21 intended recipient of the notice actually received the notice

22 and understands its contents.

23   (d) Receipt and acknowledgment.--Each recipient of the

24 notice under this section shall sign the acknowledgment and

25 return it to the appropriate educational entity as soon as

26 possible.

27   (e) Maintenance.--An educational entity shall maintain on

28 file, electronically or otherwise, each signed acknowledgment

29 received under this section.

30 § 523. Disclosure by educational entity.

1 (a) Conditions for disclosure.--An educational entity may

2 not disclose student data unless the disclosure is:

3   (1) authorized in writing by an eligible student or a

4 student's parent or legal guardian if the student is under 18

5 years of age;

6   (2) authorized or required by Federal or State law;

7   (3) determined to be necessary due to an imminent health

8 or safety emergency; or

9   (4) ordered by a court of competent jurisdiction.

10 (b) Financial benefit.--Except as otherwise provided under

11 this chapter, an educational entity may not release or otherwise

12 disclose student data or information in an educational record in

13 exchange for any good, product, application, service or any

14 other thing of measurable value.

15 § 524. Biometric identifiers.

16   An educational entity or third party may not collect any

17 biometric identifier on a student except as may be required by

18 law.

19 § 525. Targeted marketing.

20   Student data may not be released or used for purposes of

21 targeted marketing unless the release is absolutely necessary

22 for education progression, which may include the use of adaptive

23 educational software or any other strictly educational endeavor

24 whose sole purpose is to provide a tailored education experience

25 to the student.

26 § 526. Review and correction of educational records.

27 (a) Request for inspection.--An eligible student or a

28 student's parent or legal guardian if the student is under 18

29 years of age may request the inspection and review of the

30 student's student data or other information contained in the

student's educational records and maintained by an educational

entity or a third party.

(b) Transmittal of information.--Upon the request under

subsection (a), the educational entity or third party shall

provide the information in a timely manner and in electronic

form unless the requested information:

(1) is not maintained in electronic format, in which

case arrangements shall be made for transmittal in another

format; or

(2) cannot reasonably be made available to the

requesting individual or the reproduction of the requested

information would be unduly burdensome.

(c) Corrections and expungement.--

(1) A requesting individual under subsection (a) may

request that corrections be made to inaccurate or incomplete

information contained in the student's student data or other

educational record.

(2) A requesting individual under subsection (a) shall

have the right to expunge the student's student data or other

information contained in the student's educational record

that pertain to:

(i) an unsubstantiated accusation; or

(ii) an adjudicated matter if the student has been

found not at fault or not guilty of the charges raised.

(3) After receiving the request under this subsection,

the educational entity or third party that maintains the

information shall make the necessary changes to the student

data or other educational record and confirm the changes with

the requesting individual within 90 days of the request under

this subsection.

§ 527. Use of information by third parties.

(a) Personally identifiable student data.--A third party shall use personally identifiable student data received under a contract with an educational entity strictly for the purpose of providing the contracted product or service to the educational entity, unless a student or the student's parent affirmatively chooses to disclose the student's data for a secondary purpose.

(b) Prohibited uses.--A third party may not manage or use student data or information from an educational record obtained in the course of a contractual relationship with an educational entity to do any of the following:

(1) Conduct targeted marketing.

(2) Create a student profile except:

(i) as allowed under the terms of the contractual relationship with the educational entity; or

(ii) in furtherance of the purposes of the educational entity.

(3) Sell student data or information from an educational record.

(4) Exchange student data or information from an educational record for any goods, services or applications.

(5) Disclose student data or information from an educational record except as provided under this chapter.

(6) Impede the ability of a student, an eligible student or a student's parent or legal guardian if the student is under 18 years of age from downloading, exporting or otherwise saving or maintaining the student's student data or other information from the student's educational record.

(b.1) Limitation.--Subsection (b) shall not apply to nonprofit organizations engaging in activities to provide

1 students with higher education, scholarship or other educational

2 opportunities.

3   (c) Permissive uses.--A third-party contractor may:

4   (1) Use student data for adaptive learning or customized

5   student learning purposes.

6   (2) Market an educational application or product to a

7   student's parent or legal guardian if the student is under 18

8   years of age if the third party did not use student data,

9   shared by or collected on behalf of an educational entity, to

10   develop the educational application or product.

11   (3) Use a recommendation engine to recommend to an

12   eligible student or a student's parent or legal guardian if

13   the student is under 18 years of age any of the following:

14   (i) Content that relates to learning or employment,

15   within the third party's internal application, if the

16   recommendation is not motivated by payment or other

17   consideration from another party.

18   (ii) Services that relate to learning or employment,

19   within the third party's internal application, if the

20   recommendation is not motivated by payment or other

21   consideration from another party.

22   (4) Respond to an eligible student or a student's parent

23   or legal guardian if the student is under 18 years of age

24   regarding a request for information or feedback, if the

25   content of the response is not motivated by payment or other

26   consideration from another party.

27   (5) Use student data to allow or improve operability and

28   functionality of the third party's internal application.

29   (6) Disclose a student's personally identifiable

30   information at the student's request to institutions of

1 higher education and other educational organizations,

2 including scholarship providers.

3 (7) Disclose and utilize personally identifiable

4 information and aggregate student data when used solely for

5 research purposes that are compatible with the context in

6 which the information was collected.

7 § 528. Third-party contracts.

8 When contracting with a third party, an educational entity

9 shall require the following provisions in the contract:

10 (1) Requirements and restrictions related to the

11 collection, use, storage or sharing of student data by the

12 third party that are necessary for the educational entity to

13 ensure compliance with the provisions of this chapter and

14 other State law.

15 (2) A description of a person, or type of person,

16 including an affiliate or subcontractor of the third party,

17 with whom the third party may share student data or other

18 information.

19 (3) When and how to delete student data or other

20 information received by the third party.

21 (4) A prohibition on the secondary use of personally

22 identifiable student data by the third party except when used

23 for research purposes or for legitimate educational interests

24 compatible with the context in which the personal information

25 was collected.

26 (5) An agreement by the third party that the educational

27 entity or the educational entity's designee may audit the

28 third party to verify compliance with the contract.

29 (6) Requirements for the third party or a subcontractor

30 of the third party to effect security measures to prevent,

1 detect or mitigate a data breach.

2   (7) Requirements for the third party or a subcontractor

3 of the third party to notify the educational entity of a

4 suspected data breach or intrusion.

5 § 529. Law enforcement.

6   As authorized by law or court order, a third party shall

7 share student data as requested by law enforcement.

8 § 530. Exception for use of personally identifiable student

9   data.

10   Notwithstanding any provision of this chapter to the

11 contrary, this chapter does not apply to nonprofit organizations

12 using the student data for legitimate educational interests,

13 including, but not limited to, engaging in activities to provide

14 students higher education and scholarship opportunities or

15 prohibit the use of the student's personally identifiable

16 student data to identify for the student institutions of higher

17 education or scholarship providers that are seeking students who

18 meet specific criteria, provided a written data authorization by

19 the student or a student's parent or legal guardian if the

20 student is under 18 years of age permits the use. This section

21 shall apply regardless of whether the identified institutions of

22 higher education or scholarship providers provide consideration

23 to the school services contract provider.

24   SUBCHAPTER D

25   ENFORCEMENT

26 Sec.

27 541. Data breach or security compromise.

28 542. Funding.

29 543. Civil and administrative penalties.

30 544. Effect on criminal liability.

1 § 541. Data breach or security compromise.

2   (a) Notification of chief data privacy officer.--An

3 educational entity shall notify the chief data privacy officer

4 within the department of a suspected or confirmed data breach or

5 security compromise within 24 hours of becoming aware of the

6 data breach or security compromise.

7   (b) Notification of students, parents and legal guardians.--

8 If there is an unauthorized release or compromise of student

9 data by security breach or otherwise, the effected educational

10 entity shall, within three business days of verification of the

11 release or compromise, notify all of the following:

12   (1) Each eligible student whose information has been

13   released or compromised.

14   (2) Each student's parent or legal guardian if the

15   student is under 18 years of age and the student's

16   information has been released or compromised.

17   (c) Notification by third party.--If a suspected or

18 confirmed data breach or security compromise of student data

19 held by a third party has occurred, the third party shall:

20   (1) notify the educational entity with whom it has

21   contracted regarding the information within 24 hours of

22   becoming aware of the data breach or security compromise;

23   (2) take action to determine the scope of data breached

24   or otherwise compromised;

25   (3) update the educational entity once the full scope of

26   data breach and security compromise is known; and

27   (4) take all reasonable steps to notify the affected

28   individuals of the data breach or security compromise.

29 § 542. Funding.

30   No public funds shall be made available under an applicable

1 program to an educational entity that has a policy that denies

2 or effectively prevents an eligible student or a student's

3 parent or legal guardian if the student is under 18 years of age

4 the right to inspect, review or correct the student's student

5 record or information within the student's educational record.

6 § 543. Civil and administrative penalties.

7 An educational entity or third party that fails to comply

8 with any duty or other provision under this chapter resulting in

9 the intentional, knowing, reckless or negligent data breach or

10 security compromise shall be subject to the following penalties:

11 (1) Civil penalties, which shall include the following:

12 (i) The costs of identity protection for each

13 individual affected by the data breach or security

14 compromise.

15 (ii) Legal fees and costs incurred by each

16 individual affected by the data breach or security

17 compromise.

18 (iii) Any other penalty that the court deems

19 reasonable or appropriate.

20 (2) Administrative penalties by the department, which

21 shall include a fine of not less than $1,000 nor more than

22 $5,000 for each offense committed. The aggregate amount of

23 fines under this paragraph may not exceed $1,000,000 in any

24 calendar year.

25 § 544. Effect on criminal liability.

26 Nothing in this subchapter shall be construed to limit,

27 preclude or supersede criminal liability as may be applicable to

28 or enforceable under this chapter.

29 Section 2. This act shall take effect as follows:

30 (1) The following shall take effect August 1, 2024:

1   (i) The addition of 24 Pa.C.S. §§ 511(c) and 515.

2   (ii) The addition of 24 Pa.C.S. Ch. 5 Subchs. C and

3   D.

4   (2) This section shall take effect immediately.

5   (3) The remainder of this act shall take effect in 120

6   days.