THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1345 Session of 2017

INTRODUCED BY PHILLIPS-HILL, BAKER, V. BROWN, D. COSTA, DRISCOLL, GABLER, GROVE, KEEFER, LAWRENCE, B. MILLER, NEILSON, ORTITAY, PICKETT, RAPP, ROZZI AND ZIMMERMAN, MAY 5, 2017

AN ACT

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

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.

6 § 501. Scope of chapter.

7   This chapter relates to student data privacy and protection.

8 § 502. Legislative intent.

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

10 following:

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

12   (2) Student data shall be safeguarded.

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

14 legal guardians shall be honored, respected and protected.

15 § 503. Findings and declarations.

16   The General Assembly finds and declares as follows:

17   (1) Educational entities in this Commonwealth are

18 custodians of vast amounts of personally identifiable

19 information through their collection and maintenance of

20 student data.

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

22 essential student data shall be collected and that personal

23 information shall be protected, safeguarded, kept private and

24 only accessed or used by appropriate authorized persons.

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

26 adequate protection of student data.

27   (4) The Commonwealth lacks guarantees for the protection

28 for student data and the personally identifiable information

29 contained within that data.

30   (5) Given the vast personally identifiable student

1   information held, educational entities are prime targets for

2   data and information poaching by identity thieves and other

3   hackers.

4   (6) In emergencies, certain information should be

5   readily available to school officials and emergency personnel

6   to assist students and their families.

7   § 504. Definitions.

8   The following words and phrases when used in this chapter

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

10   context clearly indicates otherwise:

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

12   educational entity which:

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

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

15   by the educational entity;

16   (2) does not reveal personally identifiable student

17   data; and

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

19   single out or infer information about a student or device

20   used by a student.

21   "Biometric identifier." A measurable biological or

22   behavioral characteristic that can be used for automated

23   recognition of an individual. The following apply:

24   (1) The term shall include any of the following:

25   (i) A retina or iris scan.

26   (ii) A fingerprint.

27   (iii) A human biological sample.

28   (iv) A scan of the hand.

29   (v) A voice print.

30   (vi) Facial geometry.

1　　　　　(2)　The term shall not include any of the following:

2　　　　　　　(i)　A physical description, including, but not

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

4　　　　　　　(ii)　A writing sample.

5　　　　　　　(iii)　A written signature.

6　　　　　　　(iv)　Demographic data.

7　"Data authorization."　A written authorization by an eligible

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

9　is under 18 years of age to collect or share the student's

10　student data.

11　"Educational entity."　An organized education provider,

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

13　　　　　(1)　A school district of any class.

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

15　any class.

16　　　　　(3)　A public school.

17　　　　　(4)　An institution of higher education.

18　"Educational record."　Student data or other student

19　information created and maintained by an educational entity or a

20　third party.

21　"Eligible student."　A student who is:

22　　　　　(1)　18 years of age or older or an emancipated

23　individual; and

24　　　　　(2)　attending an institution of higher education.

25　"Family information."　Information regarding a student's

26　family member, including a parent or sibling, of the same or

27　similar nature to student data that is in the possession of an

28　educational entity or a third party.

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

30　　　　　(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.

(5) An accredited private or independent college or

university.

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

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

Licensed Schools Act.

"Necessary student data." Student data required by Federal

or State law to conduct the regular activities of an educational

entity.

"Personally identifiable student data." Student data that,

by itself or in connection with other information, would enable

a specific student or other individual to be reasonably

identified.

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

any class, intermediate unit, charter school, cyber charter

school or an area vocational-technical school.

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

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

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

School Code of 1949, and all branches and campuses of a State-

owned institution.

"State-related institution." The Pennsylvania State

University, including the Pennsylvania College of Technology,

the University of Pittsburgh, Temple University and Lincoln

University and their branch campuses.

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

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

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

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

5   descriptive of the student and collected and maintained at the

6   individual student level, regardless of physical, electronic or

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

8   following:

9   (1) The following information regarding the student:

10   (i) Name.

11   (ii) Date and location of birth.

12   (iii) Social Security number.

13   (iv) Gender.

14   (v) Race.

15   (vi) Ethnicity.

16   (vii) Tribal affiliation.

17   (viii) Sexual identity or orientation.

18   (ix) Migrant status.

19   (x) English language learner status.

20   (xi) Disability status.

21   (xii) Mother's maiden name.

22   (xiii) Contact information, including telephone

23   numbers, electronic mail addresses, physical addresses

24   and other distinct contact identifiers.

25   (xiv) Special education records or an applicable

26   mandate under the Individuals with Disabilities Education

27   Act (Public Law 91-230, 20 U.S.C. § 1400 et seq.).

28   (xv) An individualized education program or other

29   written education plan, including special education

30   evaluation data for the program or plan.

1	(xvi) The student's identification number.
2	(xvii) Local, State or national assessment results
3	or the reason for an exception from taking a local, State
4	or national assessment.
5	(xviii) Courses taken and completed, credits earned
6	or other transcript information.
7	(xix) Course grades, grade point average or another
8	indicator of academic achievement.
9	(xx) Grade level and expected graduation date.
10	(xxi) Cohort graduation rate or related information.
11	(xxii) Degree, diploma, credential attainment or
12	other school exit information.
13	(xxiii) Attendance and mobility.
14	(xxiv) Dropout data.
15	(xxv) An immunization record or the reason for an
16	exception from receiving an immunization.
17	(xxvi) Remediation efforts.
18	(xxvii) Cumulative disciplinary records.
19	(xxviii) Juvenile delinquency or dependency records.
20	(xxix) Criminal records.
21	(xxx) Medical or health records created or
22	maintained by an educational entity.
23	(xxxi) Political affiliation, voter registration
24	information or voting history.
25	(xxxii) Income or other socioeconomic information,
26	except as required by law or if an educational entity
27	determines income information is required to apply for,
28	administer, research or evaluate programs to assist
29	students from low-income families.
30	(xxxiii) Religious information or beliefs.

1   (xxxiv) A biometric identifier or other biometric

2   information.

3   (xxxv) Food purchases.

4   (xxxvi) Geolocation data.

5   (xxxvii) Any other information that either on its

6   own or collectively could reasonably be used to identify

7   a specific student.

8   (2) The following information regarding family members,

9   including parents and legal guardians, of the student:

10   (i) Name of family members.

11   (ii) Contact information for family members,

12   including telephone numbers, electronic mail addresses,

13   physical addresses and other distinct contact

14   identifiers.

15   (iii) Education status, an educational record or

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

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

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

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

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

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

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

23   or single search query without collection and retention of the

24   student's online activities over time.

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

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

27   includes a subsequent subcontractor that may accompany the

28   person in the provision of the good or service.

29   § 505. Effect of chapter.

30   Nothing in this chapter shall be construed to prohibit or

1 otherwise limit the ability of an educational entity from

2 reporting or making available aggregate student data or other

3 collective data for reasonable usage.

4   SUBCHAPTER B

5   POWERS AND DUTIES

6 Sec.

7 511. Chief data privacy officer.

8 512. Data inventory and data elements.

9 513. Forms.

10 514. Rules and regulations.

11 515. Educational entities.

12 § 511. Chief data privacy officer.

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

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

15 the department to assume primary responsibility for student data

16 privacy and security policy.

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

18 the department shall:

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

20   system shall be handled in full compliance with:

21   (i) this chapter;

22   (ii) the Family Educational Rights and Privacy Act

23   of 1974 (Public Law 90-247, 20 U.S.C. § 1232g) and its

24   associated regulations; and

25   (iii) other Federal and State data privacy and

26   security laws.

27   (2) Establish, publish and make easily available

28   policies necessary to assure that the use of technologies

29   sustain, enhance and do not erode privacy protections

30   relating to the use, collection and disclosure of student

1   data.

2   (3) Develop and provide to educational entities a model

3   student data privacy and security plan.

4   (4) Evaluate legislative and regulatory proposals

5   involving use, collection and disclosure of student data by

6   educational entities.

7   (5) Conduct a privacy impact assessment on legislative

8   proposals and regulations and program initiatives of the

9   department, including the type of personal information

10   collected and the number of students affected.

11   (6) Prepare an annual report to the General Assembly on

12   activities of the department that affect privacy, including

13   complaints of privacy violations, internal controls and other

14   related matters.

15   (7) Consult and coordinate with other representatives of

16   the department and the Commonwealth and other persons

17   regarding the quality, usefulness, openness and privacy of

18   data and the implementation of this chapter.

19   (8) Establish and operate a privacy incident response

20   program to ensure that each data-related incident involving

21   the department is properly reported, investigated and

22   mitigated.

23   (9) Establish a model process and policy for an eligible

24   student and a student's parent or legal guardian if the

25   student is under 18 years of age to file a complaint

26   regarding a violation of data privacy or an inability to

27   access, review or correct the student's student data or other

28   information contained in the student's educational record.

29   (10) Provide training, guidance, technical assistance

30   and outreach to build a culture of data privacy protection

1   and data security among educational entities and third

2   parties.

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

4   investigate issues of compliance with this chapter or another

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

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

7   officer shall:

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

9   reviews, documents, papers, recommendations and other

10   materials available to the educational entity or third party

11   under investigation;

12   (2) limit the investigation and any accompanying report

13   to those matters which are necessary or desirable to the

14   effective administration of this chapter; and

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

16   refer the matter to the appropriate Federal agency and

17   cooperate with any investigation by the Federal agency.

18   § 512. Data inventory and data elements.

19   The department shall create and post on its publicly

20   accessible Internet website a data inventory and dictionary of

21   data elements with definitions of individual student data fields

22   currently in the student data system, including information

23   which:

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

25   education mandates;

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

27   system with a statement regarding the purpose or reason for

28   the proposed collection; and

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

30   purpose or reason.

1 § 513. Forms.

2 The department shall develop forms, including, but not

3 limited to, the following:

4   (1) The notice of disclosure and acknowledgment under

5 section 522 (relating to notice of disclosure).

6   (2) The written data authorization to permit the

7 disclosure of information.

8 § 514. Rules and regulations.

9 The department shall promulgate rules and regulations

10 necessary to implement the provisions of this chapter.

11 § 515. Educational entities.

12 An educational entity shall:

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

14 officer within the department and taking into account the

15 specific needs and priorities of the educational entity,

16 adopt and implement reasonable security policies and

17 procedures to protect educational records and student data in

18 accordance with this chapter, to protect information from

19 unauthorized access, destruction, use, modification or

20 disclosure.

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

22 manager to fulfill the responsibilities under this section.

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

24 privacy officer under the department a data governance plan

25 addressing the protection of existing data and future data

26 records.

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

28 for the purpose of external research or evaluation.

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

30 data privacy officer within the department. Each annual

report shall include:

        (i) Any proposed changes to data security policies.

        (ii) Attempted occurrences of data security breach.

§ 521. Data ownership.

    (a) Authority of student.--A student is the owner of the student's student data and may download, export, transfer or otherwise save or maintain any document, data or other information created by the student that may be held or maintained, in whole or in part, by an educational entity.

    (b) Work or product.--Any work or intellectual product created by a student, whether for academic credit or otherwise, shall be the property of the student.

§ 522. Notice of disclosure.

    (a) Distribution.--An educational entity which collects student data, regardless of whether that information is developed and maintained as aggregate student data, shall provide to each eligible student and each student's parent or 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 of any good, product, application, service or any other

14 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

1 student's educational records and maintained by an educational

 2 entity or a third party.

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

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

 5 provide the information in a timely manner and in electronic

 6 form unless the request information:

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

 8   case arrangements shall be made for transmittal in another

 9   format; or

10   (2) cannot reasonably be made available to the

11   requesting individual or the reproduction of the requested

12   information would be unduly burdensome.

13   (c) Corrections and expungement.--

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

15   request that corrections be made to inaccurate or incomplete

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

17   educational record.

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

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

20   information contained in the student's educational record

21   that pertain to:

22   (i) an unsubstantiated accusation; or

23   (ii) an adjudicated matter if the student has been

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

25   (3) After receiving the request under this subsection,

26   the educational entity or third party that maintains the

27   information shall make the necessary changes to the student

28   data or other educational record and confirm the changes with

29   the requesting individual within 90 days of the request under

30   this subsection.

1 § 527. Use of information by third parties.

2   (a) Personally identifiable student data.--A third party

3 shall use personally identifiable student data received under a

4 contract with an educational entity strictly for the purpose of

5 providing the contracted product or service to the educational

6 entity.

7   (b) Prohibited uses.--A third party may not manage or use

8 student data or information from an educational record obtained

9 in the course of a contractual relationship with an educational

10 entity to do any of the following:

11   (1) Conduct targeted marketing.

12   (2) Create a student profile except:

13   (i) as allowed under the terms of the contractual

14   relation with the educational entity; or

15   (ii) in furtherance of the purposes of the

16   educational entity.

17   (3) Sell student data or information from an educational

18   record.

19   (4) Exchange student data or information from an

20   educational record for any goods, services or applications.

21   (5) Disclose student data or information from an

22   educational record except as provided under this chapter.

23   (6) Impede the ability of a student, an eligible student

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

25   under 18 years of age from downloading, exporting or

26   otherwise saving or maintaining the student's student data

27   or other information from the student's educational record.

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

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

30   student learning purposes.

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

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

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

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

5 develop the educational application or product.

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

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

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

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

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

11   recommendation is not motivated by payment or other

12   consideration from another party.

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

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

15   recommendation is not motivated by payment or other

16   consideration from another party.

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

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

19 regarding a request for information or feedback, if the

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

21 consideration from another party.

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

23 functionality of the third party's internal application.

24 § 528. Third party contracts.

25   When contracting with a third party, an educational entity

26 shall require the following provisions in the contract:

27   (1) Requirements and restrictions related to the

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

29 third party that are necessary for the educational entity to

30 ensure compliance with the provisions of this chapter and

1   other State law.

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

3   including an affiliate or subcontractor of the third party,

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

5   information.

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

7   information received by the third party.

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

9   identifiable student data by the third party.

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

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

12   third party to verify compliance with the contract.

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

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

15   detect or mitigate a data breach.

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

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

18   suspected data breach or intrusion.

19   § 529. Law enforcement.

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

21   share student data as requested by law enforcement.

22   SUBCHAPTER D

23   ENFORCEMENT

24   Sec.

25   531. Data breach or security compromise.

26   532. Funding.

27   533. Civil and administrative penalties.

28   534. Effect on criminal liability.

29   § 531. Data breach or security compromise.

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

1 educational entity shall notify the chief data privacy officer

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

3 security compromise within 24 hours of becoming aware of the

4 data breach or security compromise.

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

6 If there is an unauthorized release or compromise of student

7 data by security breach or otherwise, the effected educational

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

9 release or compromise, notify all of the following:

10 (1) Each eligible student whose information has been

11 released or compromised.

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

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

14 information has been released or compromised.

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

16 confirmed data breach or security compromise of student data

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

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

19 contracted regarding the information within 24 hours of

20 becoming aware of the data breach or security compromise;

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

22 or otherwise compromised;

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

24 data breach and security compromise is known; and

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

26 individuals of the data breach or security compromise.

27 § 532. Funding.

28 No public funds shall be made available under an applicable

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

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

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

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

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

4 § 533. Civil and administrative penalties.

5   An educational entity or third party that fails to comply

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

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

8 security compromise shall be subject to the following penalties:

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

10   (i) The costs of identity protection for each

11   individual affected by the data breach or security

12   compromise.

13   (ii) Legal fees and costs incurred by each

14   individual affected by the data breach or security

15   compromise.

16   (iii) Any other penalty that the court deems

17   reasonable or appropriate.

18   (2) Administrative penalties by the department, which

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

20       $5,000 for each offense committed. The aggregate amount of

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

22   calendar year.

23 § 534. Effect on criminal liability.

24   Nothing in this subchapter shall be construed to limit,

25 preclude or supersede criminal liability as may be applicable to

26 or enforceable under this chapter.

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

28   (1) This section shall take effect immediately.

29   (2) The following shall take effect August 1, 2018:

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

1   (ii) The addition of 24 Pa.C.S. Ch. 5 Subchs. C and
2   D.
3   (3) The remainder of this act shall take effect in 120
4 days.