
THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 797 Session of
2019

INTRODUCED BY PHILLIPS-HILL, FOLMER, MENSCH, J. WARD AND
A. WILLIAMS, JULY 9, 2019

REFERRED TO EDUCATION, JULY 9, 2019

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.

1 502. Legislative intent.

2 503. Findings and declarations.

3 504. Definitions.

4 505. Effect 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 for 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 shall include 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 shall not include any of the following:

1 (i) A physical description, including, but not
2 limited to, height, weight, hair color or eye color.

3 (ii) A writing sample.

4 (iii) A written signature.

5 (iv) Demographic data.

6 "Data authorization." A written authorization by a student
7 or a student's parent or legal guardian if the student is under
8 18 years of age to collect or share the student's student data.

9 "Educational entity." An organized education provider,
10 including, but not limited to, any of the following:

11 (1) A school district of any class.

12 (2) A board of school directors of a school district of
13 any class.

14 (3) A public school.

15 (4) An institution of higher education.

16 "Educational record." Student data or other student
17 information created and maintained by an educational entity or a
18 third party.

19 "Eligible student." A student who is:

20 (1) Eighteen years of age or older or an emancipated
21 individual; and

22 (2) attending an institution of higher education.

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

24 (1) A community college operating under Article XIX-A of
25 the act of March 10, 1949 (P.L.30, No.14), known as the
26 Public School Code of 1949.

27 (2) A State-owned institution.

28 (3) A State-related institution.

29 (4) Any other institution that is designated as State-
30 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 vocational-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 act of March 10, 1949 (P.L.30, No.14), known as the Public
19 School Code of 1949, and all branches and campuses of a State-
20 owned institution.

21 "State-related institution." The Pennsylvania State
22 University, including the Pennsylvania College of Technology,
23 the University of Pittsburgh, Temple University and Lincoln
24 University and their branch campuses.

25 "Student." An individual who attends a public school or
26 institution of higher education, whether enrolled on a full-
27 time, part-time, credit or noncredit basis.

28 "Student data." Information regarding a student that is
29 descriptive of the student and collected and maintained at the
30 individual student level, regardless of physical, electronic or

- 1 other media or format, including, but not limited to, any of the
2 following:
- 3 (1) The following information regarding the student:
- 4 (i) Name.
- 5 (ii) Date and location of birth.
- 6 (iii) Social Security number.
- 7 (iv) Gender.
- 8 (v) Race.
- 9 (vi) Ethnicity.
- 10 (vii) Tribal affiliation.
- 11 (viii) Sexual identity or orientation.
- 12 (ix) Migrant status.
- 13 (x) English language learner status.
- 14 (xi) Disability status.
- 15 (xii) Mother's maiden name.
- 16 (xiii) Contact information, including telephone
17 numbers, electronic mail addresses, physical addresses
18 and other distinct contact identifiers.
- 19 (xiv) Special education records or an applicable
20 mandate under the Individuals with Disabilities Education
21 Act (Public Law 91-230, 20 U.S.C. § 1400 et seq.).
- 22 (xv) An individualized education program or other
23 written education plan, including special education
24 evaluation data for the program or plan.
- 25 (xvi) The student's identification number.
- 26 (xvii) Local or State assessment results or the
27 reason for an exception from taking a local or State
28 assessment.
- 29 (xviii) Courses taken and completed, credits earned
30 or other transcript information.

1 (xix) Course grades, grade point average or another
2 indicator of academic achievement.

3 (xx) Grade level and expected graduation date.

4 (xxi) Cohort graduation rate or related information.

5 (xxii) Degree, diploma, credential attainment or
6 other school exit information.

7 (xxiii) Attendance and mobility.

8 (xxiv) Dropout data.

9 (xxv) An immunization record or the reason for an
10 exception from receiving an immunization.

11 (xxvi) Remediation efforts.

12 (xxvii) Cumulative disciplinary records.

13 (xxviii) Juvenile delinquency or dependency records.

14 (xxix) Criminal records.

15 (xxx) Medical or health records created or
16 maintained by an educational entity.

17 (xxxii) Political affiliation, voter registration
18 information or voting history.

19 (xxxiii) Income or other socioeconomic information,
20 except as required by law or if an educational entity
21 determines income information is required to apply for,
22 administer, research or evaluate programs to assist
23 students from low-income families.

24 (xxxiiii) Religious information or beliefs.

25 (xxxv) A biometric identifier or other biometric
26 information.

27 (xxxvi) Food purchases.

28 (xxxvii) Geolocation data.

29 (xxxviii) Any other information that either on its
30 own or collectively could reasonably be used to identify

1 a specific student.

2 (2) The following information regarding family members,
3 including parents and legal guardians, of the student:

4 (i) Name of family members.

5 (ii) Contact information for family members,
6 including telephone numbers, electronic mail addresses,
7 physical addresses and other distinct contact
8 identifiers.

9 (iii) Education status, an educational record or
10 student data of a family member who is a student.

11 "Targeted marketing." Advertising to a student or a
12 student's parent or guardian that is selected based on
13 information obtained or inferred from the student's online or
14 offline behavior, usage of applications or student data. The
15 term does not include advertising to a student at an online
16 location based on the student's current visit to that location
17 or single search query without collection and retention of the
18 student's online activities over time. The term does not include
19 using the student's personally identifiable student data to
20 identify for the student institutions of higher education or
21 scholarship providers that are seeking students who meet
22 specific criteria, provided a written data authorization by the
23 student, or the student's parent or legal guardian if the
24 student is under 18 years of age, permits the disclosure and
25 use.

26 "Third party." A person that enters into a contract with an
27 educational entity to provide a good or service. The term
28 includes a subsequent subcontractor that may accompany the
29 person in the provision of the good or service.

30 § 505. Effect of chapter.

1 Nothing in this chapter shall be construed to prohibit or
2 otherwise limit the ability of an educational entity from
3 reporting or making available aggregate student data or other
4 collective data for reasonable usage.

5 SUBCHAPTER B

6 POWERS AND DUTIES

7 Sec.

8 511. Chief data privacy officer.

9 512. Data inventory and data elements.

10 513. Forms.

11 514. Rules and regulations.

12 515. Educational entities.

13 § 511. Chief data privacy officer.

14 (a) Designation.--The Secretary of Education shall designate
15 an individual to serve as the chief data privacy officer within
16 the department to assume primary responsibility for student data
17 privacy and security policy.

18 (b) Specific duties.--The chief data privacy officer within
19 the department shall:

20 (1) Ensure that student data contained in the State data
21 system shall be handled in full compliance with:

22 (i) this chapter;

23 (ii) the Family Educational Rights and Privacy Act
24 of 1974 (Public Law 90-247, 20 U.S.C. § 1232g) and its
25 associated regulations; and

26 (iii) other Federal and State data privacy and
27 security laws.

28 (2) Establish, publish and make easily available
29 policies necessary to assure that the use of technologies
30 sustain, enhance and do not erode privacy protections

1 relating to the use, collection and disclosure of student
2 data.

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

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

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

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

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

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

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

30 (10) Provide training, guidance, technical assistance

1 and outreach to build a culture of data privacy protection
2 and data security among educational entities and third
3 parties.

4 (c) Investigations.--The chief data privacy officer may
5 investigate issues of compliance with this chapter or another
6 data privacy or security law concerning a matter related to this
7 chapter. In conducting the investigation, the chief data privacy
8 officer shall:

9 (1) have access to all records, reports, audits,
10 reviews, documents, papers, recommendations and other
11 materials available to the educational entity or third party
12 under investigation;

13 (2) limit the investigation and any accompanying report
14 to those matters which are necessary or desirable to the
15 effective administration of this chapter; and

16 (3) in matters related to compliance with Federal law,
17 refer the matter to the appropriate Federal agency and
18 cooperate with any investigation by the Federal agency.

19 § 512. Data inventory and data elements.

20 The department shall create and post on its publicly
21 accessible Internet website a data inventory and dictionary of
22 data elements with definitions of individual student data fields
23 currently in the student data system, including information
24 which:

25 (1) is required to be reported by Federal or State
26 education mandates;

27 (2) has been proposed for inclusion in the student data
28 system with a statement regarding the purpose or reason for
29 the proposed collection; and

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

1 purpose or reason.

2 § 513. Forms.

3 The department shall develop forms, including, but not
4 limited to, the following:

5 (1) The notice of disclosure and acknowledgment under
6 section 522 (relating to notice of disclosure).

7 (2) The written data authorization to permit the
8 disclosure of information.

9 § 514. Rules and regulations.

10 The department shall promulgate rules and regulations
11 necessary to implement the provisions of this chapter.

12 § 515. Educational entities.

13 An educational entity shall:

14 (1) Subject to the approval of the chief data privacy
15 officer within the department and taking into account the
16 specific needs and priorities of the educational entity,
17 adopt and implement reasonable security policies and
18 procedures to protect educational records and student data in
19 accordance with this chapter to protect information from
20 unauthorized access, destruction, use, modification or
21 disclosure.

22 (2) Designate an individual to act as a student data
23 manager to fulfill the responsibilities under this section.

24 (3) Create, maintain and submit to the chief data
25 privacy officer under the department a data governance plan
26 addressing the protection of existing data and future data
27 records.

28 (4) Establish a review process for all requests for data
29 for the purpose of external research or evaluation.

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

1 data privacy officer within the department. Each annual
2 report shall include:

3 (i) Any proposed changes to data security policies.

4 (ii) Attempted occurrences of data security breach.

5 SUBCHAPTER C

6 DISCLOSURE AND USE OF INFORMATION

7 Sec.

8 521. Data ownership.

9 522. Notice of disclosure.

10 523. Disclosure by educational entity.

11 524. Biometric identifiers.

12 525. Targeted marketing.

13 526. Review and correction of educational records.

14 527. Use of information by third parties.

15 528. Third-party contracts.

16 529. Law enforcement.

17 530. Exception for use of personally identifiable student data.

18 § 521. Data ownership.

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

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

27 § 522. Notice of disclosure.

28 (a) Distribution.--An educational entity which collects
29 student data, regardless of whether that information is
30 developed and maintained as aggregate student data, shall

1 provide to each eligible student and each student's parent or
2 legal guardian if the student is under 18 years of age an annual
3 written notice outlining the conditions under which the
4 student's student data may be disclosed.

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

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

7 (2) annually updated and distributed; and

8 (3) written in plain language that is easily

9 comprehended by an average individual.

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

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

12 the educational entity collects and the rationale for the

13 collection of the data;

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

15 without a written data authorization by the eligible student

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

17 under 18 years of age;

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

19 student data under a contractual agreement;

20 (4) outline the rights and responsibilities under this

21 chapter; and

22 (5) contain an acknowledgment specifying that the

23 intended recipient of the notice actually received the notice

24 and understands its contents.

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

26 notice under this section shall sign the acknowledgment and

27 return it to the appropriate educational entity as soon as

28 possible.

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

30 file, electronically or otherwise, each signed acknowledgment

1 received under this section.

2 § 523. Disclosure by educational entity.

3 (a) Conditions for disclosure.--An educational entity may
4 not disclose student data unless the disclosure is:

5 (1) authorized in writing by an eligible student or a
6 student's parent or legal guardian if the student is under 18
7 years of age;

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

9 (3) determined to be necessary due to an imminent health
10 or safety emergency; or

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

12 (b) Financial benefit.--Except as otherwise provided under
13 this chapter, an educational entity may not release or otherwise
14 disclose student data or information in an educational record in
15 exchange of any good, product, application, service or any other
16 thing of measurable value.

17 § 524. Biometric identifiers.

18 An educational entity or third party may not collect any
19 biometric identifier on a student except as may be required by
20 law.

21 § 525. Targeted marketing.

22 Student data may not be released or used for purposes of
23 targeted marketing unless the release is absolutely necessary
24 for education progression, which may include the use of adaptive
25 educational software or any other strictly educational endeavor
26 whose sole purpose is to provide a tailored education experience
27 to the student.

28 § 526. Review and correction of educational records.

29 (a) Request for inspection.--An eligible student or a
30 student's parent or legal guardian if the student is under 18

1 years of age may request the inspection and review of the
2 student's student data or other information contained in the
3 student's educational records and maintained by an educational
4 entity or a third party.

5 (b) Transmittal of information.--Upon the request under
6 subsection (a), the educational entity or third party shall
7 provide the information in a timely manner and in electronic
8 form unless the request information:

9 (1) is not maintained in electronic format, in which
10 case arrangements shall be made for transmittal in another
11 format; or

12 (2) cannot reasonably be made available to the
13 requesting individual or the reproduction of the requested
14 information would be unduly burdensome.

15 (c) Corrections and expungement.--

16 (1) A requesting individual under subsection (a) may
17 request that corrections be made to inaccurate or incomplete
18 information contained in the student's student data or other
19 educational record.

20 (2) A requesting individual under subsection (a) shall
21 have the right to expunge the student's student data or other
22 information contained in the student's educational record
23 that pertain to:

24 (i) an unsubstantiated accusation; or

25 (ii) an adjudicated matter if the student has been
26 found not at fault or not guilty of the charges raised.

27 (3) After receiving the request under this subsection,
28 the educational entity or third party that maintains the
29 information shall make the necessary changes to the student
30 data or other educational record and confirm the changes with

1 the requesting individual within 90 days of the request under
2 this subsection.

3 § 527. Use of information by third parties.

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

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

14 (1) Conduct targeted marketing.

15 (2) Create a student profile except:

16 (i) as allowed under the terms of the contractual
17 relation with the educational entity; or

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

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

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

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

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

1 (b.1) Limitation.--Subsection (b) shall not apply to
2 nonprofit organizations engaging in activities to provide
3 students with higher education, scholarship or other educational
4 opportunities.

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

6 (1) Use student data for adaptive learning or customized
7 student learning purposes.

8 (2) Market an educational application or product to a
9 student's parent or legal guardian if the student is under 18
10 years of age if the third party did not use student data,
11 shared by or collected on behalf of an educational entity, to
12 develop the educational application or product.

13 (3) Use a recommendation engine to recommend to an
14 eligible student or a student's parent or legal guardian if
15 the student is under 18 years of age any of the following:

16 (i) Content that relates to learning or employment,
17 within the third party's internal application, if the
18 recommendation is not motivated by payment or other
19 consideration from another party.

20 (ii) Services that relate to learning or employment,
21 within the third party's internal application, if the
22 recommendation is not motivated by payment or other
23 consideration from another party.

24 (4) Respond to an eligible student or a student's parent
25 or legal guardian if the student is under 18 years of age
26 regarding a request for information or feedback, if the
27 content of the response is not motivated by payment or other
28 consideration from another party.

29 (5) Use student data to allow or improve operability and
30 functionality of the third party's internal application.

1 (6) Disclose a student's personally identifiable
2 information at the student's request to institutions of
3 higher education and other educational organizations,
4 including scholarship providers.

5 (7) Disclose and utilize personally identifiable
6 information and aggregate student data when used solely for
7 research purposes that are compatible with the context in
8 which the information was collected.

9 § 528. Third-party contracts.

10 When contracting with a third party, an educational entity
11 shall require the following provisions in the contract:

12 (1) Requirements and restrictions related to the
13 collection, use, storage or sharing of student data by the
14 third party that are necessary for the educational entity to
15 ensure compliance with the provisions of this chapter and
16 other State law.

17 (2) A description of a person, or type of person,
18 including an affiliate or subcontractor of the third party,
19 with whom the third party may share student data or other
20 information.

21 (3) When and how to delete student data or other
22 information received by the third party.

23 (4) A prohibition on the secondary use of personally
24 identifiable student data by the third party except when used
25 for research purposes or for legitimate educational interests
26 compatible with the context in which the personal information
27 was collected.

28 (5) An agreement by the third party that the educational
29 entity or the educational entity's designee may audit the
30 third party to verify compliance with the contract.

1 (6) Requirements for the third party or a subcontractor
2 of the third party to effect security measures to prevent,
3 detect or mitigate a data breach.

4 (7) Requirements for the third party or a subcontractor
5 of the third party to notify the educational entity of a
6 suspected data breach or intrusion.

7 § 529. Law enforcement.

8 As authorized by law or court order, a third party shall
9 share student data as requested by law enforcement.

10 § 530. Exception for use of personally identifiable student
11 data.

12 Notwithstanding any provision of this chapter to the
13 contrary, this chapter does not apply to nonprofit organizations
14 using the student data for legitimate educational interests,
15 including, but not limited to, engaging in activities to provide
16 students higher education and scholarship opportunities or
17 prohibit the use of the student's personally identifiable
18 student data to identify for the student institutions of higher
19 education or scholarship providers that are seeking students who
20 meet specific criteria, provided a written data authorization by
21 the student or a student's parent or legal guardian if the
22 student is under 18 years of age permits the use. This section
23 shall apply regardless of whether the identified institutions of
24 higher education or scholarship providers provide consideration
25 to the school services contract provider.

26 SUBCHAPTER D

27 ENFORCEMENT

28 Sec.

29 541. Data breach or security compromise.

30 542. Funding.

1 543. Civil and administrative penalties.

2 544. Effect on criminal liability.

3 § 541. Data breach or security compromise.

4 (a) Notification of chief data privacy officer.--An
5 educational entity shall notify the chief data privacy officer
6 within the department of a suspected or confirmed data breach or
7 security compromise within 24 hours of becoming aware of the
8 data breach or security compromise.

9 (b) Notification of students, parents and legal guardians.--
10 If there is an unauthorized release or compromise of student
11 data by security breach or otherwise, the effected educational
12 entity shall, within three business days of verification of the
13 release or compromise, notify all of the following:

14 (1) Each eligible student whose information has been
15 released or compromised.

16 (2) Each student's parent or legal guardian if the
17 student is under 18 years of age and the student's
18 information has been released or compromised.

19 (c) Notification by third party.--If a suspected or
20 confirmed data breach or security compromise of student data
21 held by a third party has occurred, the third party shall:

22 (1) notify the educational entity with whom it has
23 contracted regarding the information within 24 hours of
24 becoming aware of the data breach or security compromise;

25 (2) take action to determine the scope of data breached
26 or otherwise compromised;

27 (3) update the educational entity once the full scope of
28 data breach and security compromise is known; and

29 (4) take all reasonable steps to notify the affected
30 individuals of the data breach or security compromise.

1 § 542. Funding.

2 No public funds shall be made available under an applicable
3 program to an educational entity that has a policy that denies
4 or effectively prevents an eligible student or a student's
5 parent or legal guardian if the student is under 18 years of age
6 the right to inspect, review or correct the student's student
7 record or information within the student's educational record.

8 § 543. Civil and administrative penalties.

9 An educational entity or third party that fails to comply
10 with any duty or other provision under this chapter resulting in
11 the intentional, knowing, reckless or negligent data breach or
12 security compromise shall be subject to the following penalties:

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

14 (i) The costs of identity protection for each
15 individual affected by the data breach or security
16 compromise.

17 (ii) Legal fees and costs incurred by each
18 individual affected by the data breach or security
19 compromise.

20 (iii) Any other penalty that the court deems
21 reasonable or appropriate.

22 (2) Administrative penalties by the department, which
23 shall include a fine of not less than \$1,000 nor more than
24 \$5,000 for each offense committed. The aggregate amount of
25 finest under this paragraph may not exceed \$1,000,000 in any
26 calendar year.

27 § 544. Effect on criminal liability.

28 Nothing in this subchapter shall be construed to limit,
29 preclude or supersede criminal liability as may be applicable to
30 or enforceable under this chapter.

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

2 (1) This section shall take effect immediately.

3 (2) The following shall take effect August 1, 2020:

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

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

6 D.

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

8 days.