PRINTER'S NO. 18

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 37 Session of 2021

INTRODUCED BY PHILLIPS-HILL, J. WARD AND MENSCH, JANUARY 20, 2021

REFERRED TO EDUCATION, JANUARY 20, 2021

AN ACT

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

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Part I of Title 24 of the Pennsylvania Consolidated Statutes is amended by adding a chapter to read:

CHAPTER 5

STUDENT DATA PRIVACY AND PROTECTION

Subchapter

A. General Provisions

B. Powers and Duties

C. Disclosure and Use of Information

D. Enforcement

SUBCHAPTER A

GENERAL PROVISIONS

Sec.

501. Scope of chapter.

§ 501. Scope of chapter.

This chapter relates to student data privacy and protection.

§ 502. Legislative intent.

It is the intent of the General Assembly to ensure the following:

(1) Only essential student data shall be collected.

(2) Student data shall be safeguarded.

(3) The privacy rights of students and their parents or legal guardians shall be honored, respected and protected.

§ 503. Findings and declarations.

The General Assembly finds and declares as follows:

(1) Educational entities in this Commonwealth are custodians of vast amounts of personally identifiable information through their collection and maintenance of student data.

(2) It is critically important to ensure that only essential student data shall be collected and that personal information shall be protected, safeguarded, kept private and only accessed or used by appropriate authorized persons.

(3) The Commonwealth lacks a sufficient plan to ensure adequate protection of student data.

(4) The Commonwealth lacks guarantees for the protection of student data and the personally identifiable information contained within that data.

(5) Given the vast personally identifiable student information held, educational entities are prime targets for

data and information poaching by identity thieves and other hackers.

(6) In emergencies, certain information should be readily available to school officials and emergency personnel to assist students and their families.

§ 504. Definitions.

The following words and phrases when used in this chapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Aggregate student data." Student data collected by an educational entity which:

(1) is totaled and reported at the group, cohort, school, school district, region or State level as determined by the educational entity;

(2) does not reveal personally identifiable student data; and

(3) cannot reasonably be used to identify, contact, single out or infer information about a student or device used by a student.

"Biometric identifier." A measurable biological or behavioral characteristic that can be used for automated recognition of an individual. The following apply:

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

(i) A retina or iris scan.

(ii) A fingerprint.

(iii) A human biological sample.

(iv) A scan of the hand.

(v) A voice print.

(vi) Facial geometry.

(2) The term shall 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.

(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 career and technical school.

"State-owned institution." An institution which is part of the State System of Higher Education under Article XX-A of 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.

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

"Student data." Information regarding a student that is descriptive of the student and collected and maintained at the individual student level, regardless of physical, electronic or 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 the Individuals with Disabilities Education Act (Public Law 91-230, 20 U.S.C. § 1400 et seq.).

(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

indicator of academic achievement.

(xx) Grade level and expected graduation date.

(xxi) Cohort graduation rate or related information.

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

(xxiii) Attendance and mobility.

(xxiv) Dropout data.

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

(xxvi) Remediation efforts.

(xxvii) Cumulative disciplinary records.

(xxviii) Juvenile delinquency or dependency records.

(xxix) Criminal records.

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

(xxxi) Political affiliation, voter registration information or voting history.

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

(xxxiii) Religious information or beliefs.

(xxxiv) A biometric identifier or other biometric information.

(xxxv) Food purchases.

(xxxvi) Geolocation data.

(xxxvii) Any other information that either on its own or collectively could reasonably be used to identify a specific student.

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

(i) Name of family members.

(ii) Contact information for family members, including telephone numbers, email addresses, physical addresses and other distinct contact identifiers.

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

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

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

§ 505. Effect of chapter.

Nothing in this chapter shall be construed to prohibit or otherwise limit the ability of an educational entity from

reporting or making available aggregate student data or other collective data for reasonable usage.

SUBCHAPTER B

POWERS AND DUTIES

Sec.

§ 511. Chief data privacy officer.

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

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

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

(i) this chapter;

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

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

(2) Establish, publish and make easily available policies necessary to assure that the use of technologies sustain, enhance and do not erode privacy protections relating to the use, collection and disclosure of student 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

parties.

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

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

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

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

§ 512. Data inventory and data elements.

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

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

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

(3) the department collects or maintains with no current purpose or reason.

§ 513. Forms.

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

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

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

§ 514. Rules and regulations.

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

§ 515. Educational entities.

An educational entity shall:

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

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

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

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

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

SUBCHAPTER C

DISCLOSURE AND USE OF INFORMATION

Sec.

§ 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

written notice outlining the conditions under which the student's student data may be disclosed.

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

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

(2) annually updated and distributed; and

(3) written in plain language that is easily comprehended by an average individual.

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

(1) list the necessary and optional student data which the educational entity collects and the rationale for the collection of the data;

(2) state that student data collected may not be shared without a written data authorization by the eligible student or a student's parent or legal guardian if the student is under 18 years of age;

(3) list each third party with access or control of student data under a contractual agreement;

(4) outline the rights and responsibilities under this chapter; and

(5) contain an acknowledgment specifying that the intended recipient of the notice actually received the notice and understands its contents.

(d) Receipt and acknowledgment.--Each recipient of the notice under this section shall sign the acknowledgment and return it to the appropriate educational entity as soon as possible.

(e) Maintenance.--An educational entity shall maintain on file, electronically or otherwise, each signed acknowledgment received under this section.

§ 523. Disclosure by educational entity.

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

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

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

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

(4) ordered by a court of competent jurisdiction.

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

§ 524. Biometric identifiers.

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

§ 525. Targeted marketing.

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

§ 526. Review and correction of educational records.

(a) Request for inspection.--An eligible student or a student's parent or legal guardian if the student is under 18 years of age may request the inspection and review of the 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

students with higher education, scholarship or other educational opportunities.

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

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

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

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

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

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

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

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

(6) Disclose a student's personally identifiable information at the student's request to institutions of

higher education and other educational organizations, including scholarship providers.

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

§ 528. Third-party contracts.

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

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

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

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

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

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

(6) Requirements for the third party or a subcontractor of the third party to effect security measures to prevent,

detect or mitigate a data breach.

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

§ 529. Law enforcement.

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

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

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

SUBCHAPTER D

ENFORCEMENT

Sec.

§ 541. Data breach or security compromise.

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

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

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

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

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

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

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

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

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

§ 542. Funding.

No public funds shall be made available under an applicable

program to an educational entity that has a policy that denies or effectively prevents an eligible student or a student's parent or legal guardian if the student is under 18 years of age the right to inspect, review or correct the student's student record or information within the student's educational record.

§ 543. Civil and administrative penalties.

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

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

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

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

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

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

§ 544. Effect on criminal liability.

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

Section 2. This act shall take effect as follows:

(1) This section shall take effect immediately.

(2) The following shall take effect August 1, 2022:

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

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

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