HB 1586-FN – AS INTRODUCED

2014 SESSION

14-2230
04/10

HOUSE BILL ***1586-FN***

AN ACT relative to student and teacher information protection and privacy.

SPONSORS: Rep. Cordelli, Carr 4; Rep. Boehm, Hills 20; Rep. Bick, Rock 8; Rep. Gorman, Hills 31; Rep. Marston, Hills 19; Rep. Shaw, Hills 16; Rep. Hoell, Merr 23

COMMITTEE: Education

ANALYSIS

This bill establishes procedures for protecting the privacy of student and teacher personally-identifiable data. The bill also prohibits the use of video monitoring in a classroom for the purpose of teacher evaluations, affective computing methods, predictive modeling, radio frequency identification devices, and remote surveillance software on school laptops and tablets, without the written consent of a parent or legal guardian.

- -

Explanation: Matter added to current law appears in ***bold italics.***
Matter removed from current law appears [~~in brackets and struckthrough.~~]
Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

HB 1586-FN – AS INTRODUCED

14-2230
04/10

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Fourteen

AN ACT relative to student and teacher information protection and privacy.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 New Subdivision; School Boards; Student and Teacher Information Protection and Privacy. Amend RSA 189 by inserting after section 64 the following new subdivision:

Student and Teacher Information Protection and Privacy

189:65 Definitions. In this subdivision:

I. "Affective computing" means systems and devices that attempt to recognize, interpret, process, and simulate aspects of human feelings or emotions.

II. "Biometric" means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

III. "Board" means the state board of education.

IV. "Department" means the department of education.

V. "Data security breach" means the security, confidentiality, or integrity of any encrypted or unencrypted student or teacher personally identifiable data was, or is reasonably believed to have been, acquired by an unauthorized person from any student or teacher database.

VI. "Disclosure" means permitting access to, revealing, releasing, transferring, or otherwise communicating, personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic.

VII. "FERPA" means the Family Education Rights and Privacy Act (20 U.S.C 1232g).

VIII. "Predictive modeling" means use of educational data mining methods used to make predictions about future behaviors or performance.

IX. "Statewide longitudinal data system" (SLDS) means the department's statewide longitudinal data system containing student information and any other state or federal database, excluding special education or adult education, containing student information, whether under contract to, or with a memorandum of understanding with, the department.

X. "Student personally-identifiable data" or "student-level data" means:

(a) The student's name.

(b) The name of the student's parents or other family members.

(c) The address of the student or student's family.

(d) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal

knowledge of the relevant circumstances, to identify the student with reasonable certainty.

(e) Information requested by a person who the department reasonably believes knows the identity of the student to whom the education record relates.

XI. "Teacher database" means any database containing information on teachers, principals, paraprofessionals, and other administrators.

XII. "Teacher personally-identifiable data" or "teacher data," which shall apply to paraprofessionals, principals, and other administrators, means:

(a) The teacher's social security number.

(b) Date of birth.

(c) Street address.

(d) Email address.

(e) Compensation information.

(f) Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

(g) Information requested by a person who the department reasonably believes or knows the identity of the student to whom the education record relates.

XIII. "Workforce information" means information related to unemployment insurance, wage records, unemployment benefit claims, or employment and earnings data from workforce data sources, such as state wage records, wage record interchange system (WRIS), or the Federal Employment Data Exchange System (FEDES).

189:66 Data Inventory and Policies Publication.

I. The department shall create, maintain, and make publicly available on the department's website, a data element dictionary containing definitions of all data fields currently in the SLDS or any other database maintained by the department..

II. The department shall develop and make public on the department's website policies and procedures to ensure compliance with FERPA and applicable state law, including but not limited to:

(a) Department policies for online/web access to any department database containing any student personally-identifiable data;

(b) Department data breach response policy;

(c) Department criteria for the approval of research and data requests from state and local agencies, the general court, researchers, and the public; or

(d) Students and parents rights under FERPA and applicable state law including:

(1) The right to inspect and review the student's education records within 14 days after the day the school receives a request for access;

(2) The right to request the amendment of the student's education records that the

parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA;

(3) The right to provide written consent before the school discloses student personally-identifiable data from the student's education records, as provided in applicable state and federal law, and

(4) The right to file a complaint with the Family Policy Compliance Office in the United States Department of Education concerning alleged failures to comply with the requirements of FERPA.

189:67 Data Security Planning.

I. The department shall develop a detailed data security plan that will be presented to the board, the legislative oversight committee established in RSA 193-C:7, and the commissioner of the department of information technology. The plan shall include:

(a) Guidelines for authorizing access to the student data system and to individual student data including guidelines for authentication of authorized access;

(b) Privacy compliance standards,

(c) Privacy and security audits,

(d) Breach planning, notification and procedures, and

(e) Data retention and disposition policies;

II. The department shall:

(a) Notify, as soon as practicable, any teacher or student whose personally-identifiable information could reasonably be assumed to have been part of any data security breach, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the integrity of the data system.

(b) Issue an annual data security breach report to the governor, state board, senate president, speaker of the house of representatives, chairperson of the house committee with primary jurisdiction over education, legislative oversight committee established in RSA 193-C:7, and the commissioner of the department of information technology. The breach report shall also be posted to the department website and shall not include any information that itself would pose a security threat to a database or data system. The report shall include:

(1) The name of the organization reporting the breach.

(2) The types of personal information that were or are reasonably believed to have been the subject of a breach.

(3) The date, estimated date, or date range of the breach.

(4) A general description of the breach incident.

(5) The estimated number of students and/or teachers affected by the breach.

(6) Information about what the reporting organization has done to protect individuals whose information has been breached.

189:68 Limits on Disclosure of Information,

I. The department or a local school shall disclose student personally identifiable data about a student to the parent of the student or to the eligible student in accordance with FERPA and applicable state law.

II. The department may disclose teacher-personally-identifiable data or student personally-identifiable data with the written consent of the teacher, or parent of the student, or the eligible student in accordance with FERPA if the disclosure is to a nonprofit organization provided:

(a) The organization states in writing that it seeks the information for a specific identified purpose determined by the school to be in the educational interest of the student and that the organization states in writing that it will use the information only for the specific identified purpose and will return or destroy the information when the purpose has been fulfilled, but not later than one year after receipt.

(b) The organization states in writing that it has not used or disclosed student personally identifiable data from any school in a manner inconsistent with the terms of disclosure within the past 5 years, that it will not disclose such data, and it agrees that ownership of the data shall remain with the department;

(c) The department has no reason to believe that the recipient used or disclosed student personally-identifiable data from any school in a manner inconsistent with the terms of the disclosure within the past 5 years; and

(d) The department makes available on the department website the agreement including the information to be released, release date, the purpose of release, under which FERPA provision the release is authorized, and how and when data is to be destroyed by the receiving organization.

III. The department shall not disclose teacher personally-identifiable data or student personally-identifiable data, even with the consent of the parent, teacher, or of the student or the eligible student, for any commercial or for-profit activity, including but not limited to use for:

(a) Marketing products or services;

(b) Selling or renting student or teacher personally-identifiable data for use in marketing products or services;

(c) Creating, correcting, or updating an individual or household profile;

(d) Compilation of a list of students; or

(e) Any other purpose considered by the school as likely to be a commercial, for-profit activity.

IV. The department, or any organization under contract to or with a memorandum of understanding with the department, shall not disclose teacher or student personally-identifiable data to any federal department or agency unless pursuant to a court order or subpoena.

V. Student or teacher data may be shared with any assessment consortium or assessment contractor of which the state is a member only when:

(a) No student personally-identifiable data or teacher personally-identifiable data is shared, other than for purposes of test taking verification;

(b) The data are limited to information directly related to the assessment of student knowledge and skills; and

(c) The organization states in writing that it will not disclose the data.

VI. The department or a local school shall only disclose the minimum amount of data necessary to accomplish the purpose of the request.

189:69 Student and Teacher Privacy.

I. The department shall not collect or maintain any of the following data in any student database:

(a) Juvenile delinquency records.

(b) Criminal records.

(c) Medical and dental insurance information.

(d) Student birth information, other than date of birth and place of birth.

(e) Student Social Security number.

(f) Student biometric information.

(g) Student postsecondary workforce information.

(h) Height and weight.

(i) Body mass index (BMI).

(j) Political affiliations or beliefs of student or parents.

(k) Family income.

(1) Mother's maiden name.

(m) Parent's social security numbers.

(n) Mental and psychological problems of the student or the student's family.

(o) Sex behavior or attitudes.

(p) Indication of a student pregnancy.

(q) Religious practices, affiliations, or beliefs of the student or the student's parents.

II. A school board shall adopt a policy regulating video monitoring of classrooms for the purpose of teacher evaluations requiring school board approval, after a public hearing, and the written consent of the teacher and the parent or legal guardian of an affected student.

III. No student database shall be used for predictive modeling for detecting behaviors, beliefs, or value systems, or predicting or forecasting student outcomes.

IV. No school shall use affective computing methods including, but not limited to, analysis of facial expressions, EEG brain wave patterns, skin conductance, heart rate variability, posture, and eye-tracking without approval of the school board, after a public hearing, and written notification to the parent or legal guardian of an affected student. The school board shall adopt a policy providing that no affective computing methods shall be permitted unless a parent or legal guardian consents in

writing to participate in such methods.

V. No school shall require a student to use an identification device that uses radio frequency identification, or similar technology, to identify the student, transmit information regarding the student, or monitor or track the student without approval of the school board, after a public hearing, and notification to the parent or legal guardian of an affected student. The school board shall adopt a policy providing that use of a radio frequency identification device shall not be permitted unless the parent or legal guardian of an affected student consents in writing to its use.

VI. No school shall install remote camera surveillance software on a school supplied computing device provided to a student or a teacher without the approval of the school board, after a public hearing. A school board that provides computing devices to students or teachers shall adopt a policy prohibiting the use of remote camera surveillance software on a school supplied computing device without the written consent of the teacher or a parent or legal guardian of the affected student.

2 Information Technology Council; Members; Commissioner of Education. RSA 21-R:6, II(g) is repealed and reenacted to read as follows:

(g) The commissioner of the department of education, or designee.

3 New Paragraphs; Duties of Legislative Oversight Committee. Amend RSA 193-C:8 by inserting after paragraph X the following new paragraphs:

XI. Receive the data security plan and annual data security breach report required under RSA 189:67 from the department of education.

XII. Evaluate and review existing department of education data security plans, and propose legislation for strengthening data security for student and teachers, as necessary.

4 Effective Date. This act shall take effect 60 days after its passage.

LBAO
14-2230
12/13/13

HB 1586-FN - FISCAL NOTE

AN ACT relative to student and teacher information protection and privacy.

FISCAL IMPACT:

The Department of Education and Department of Information Technology state this bill, **as introduced**, will increase state and local expenditures by an indeterminable amount in FY 2015 and each year thereafter. There will be no impact on state, county, and local revenue, or county expenditures.

METHODOLOGY:

The Department of Education states this bill establishes procedures for protecting the privacy of student and teacher personally-identifiable data. The Department assumes it would need to hire a part-time staff person to oversee the reporting requirements set forth in this bill as well as contract with a consultant to assist with the initial development of policy and procedure manuals. The Department estimates these costs to be as follows:

	FY 2015	FY 2016	FY 2017	FY 2018
Part-Time Staff	$38,005	$38,005	$38,005	$38,005
Consulting Services	$60,000	$0	$0	$0
Total	**$98,005**	**$38,005**	**$38,005**	**$38,005**

The Department states this bill, as written, has conflicts with state and federal law, which could jeopardize millions of dollars in federal education aid to the state. The Department states this bill would also require an effort from local towns in terms of school board oversight and public hearings, to which the Department is unable to estimate a fiscal impact.

The Department of Information Technology states this bill would necessitate a significant information technology related effort. The Department states it would need to work with the Department of Education to create a data dictionary to meet the requirements set forth in this bill as the Department of Education current databases would not be adequate. The Department of Information Technology estimates it would take two full-time consultants working with existing Department of Education staff for approximately one year to create an adequate data dictionary. The estimated cost for such consulting services is $320,000 in FY 2015 (2 consultants @ $80/hour for 2,000 hours each).