Comments on proposed regulations for NYS student privacy law Education Law §2-d

March 27, 2019

Submitted by the Parent Coalition for Student Privacy, New York State Allies for Public Education and Class Size Matters by email: REGCOMMENTS@nysed.gov

Proposed regulations posted here: http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/proposed-part-121-for-pii.pdf
Deadline for comments March 31, 2019

Summary:

- In the Parent Bill of Rights, the following federal laws that afford parents and their children important rights to privacy must be included: **Protection of Pupil Rights Amendment** (PPRA), **National School Lunch Act** (NSLA) and **Children's Online Privacy Protection Act** (*COPPA*) . Each of these laws provide parents with rights to protect their children's personal data and is inexplicable why they have been omitted from the NYSED Parent Bill of Rights and the Student Privacy website for so long, especially as Education Law §2-d states that the Parent bill of rights shall include **all "***State and federal laws [that] protect the confidentiality of personally identifiable information.*"

- The Education Law §2-d also states that "*The chief privacy officer, with input from parents and other education and expert stakeholders, shall develop additional elements of the parents bill of rights for data privacy and security. The commissioner shall promulgate regulations for a comment period whereby parents and other members of the public may submit comments and suggestions to the chief privacy officer to be considered for inclusion*." This clause should be included in the regulations as over time there will likely be more threats to student privacy as districts contract with additional vendors collecting personal student data in digital form.

- The personal information of former students and former teachers as well as current students and teachers should be explicitly protected and covered by the regulations.

- The state should not be collecting the personally identifiable data on individual students regarding to their country of birth or their in-school or out-of-school suspensions, given the extreme sensitivity of this data. If necessary, both categories of information can be reported to the state by districts in an aggregate basis and if the state is worried about its accuracy, this reporting should be audited.

- The regulations omit specific provisions in Education Law §2-d, including that school districts shall not report to the department the following student data elements:(1) juvenile delinquency records;(2) criminal records;(3) medical and health records; and(4) student biometric information unless required by law except in the case of law or required educational enrollment data. This should be added.

- The words "license" should be added to the section on the Parent Bill of Rights and in the section on prohibiting the selling of data by districts or their vendors. The latter provision should read as follows "*Personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold, licensed or used for marketing purposes.*" There is no significant difference between selling and licensing data, and yet College Board exploits an unacceptable loophole, claiming they so not sell student data but instead "license" it for a fee to other companies and organizations, even as the US Department of Education points out that they are really selling it.

- Each educational agency should publish its data security and privacy policy on its website and provide notice of these policies to parents, not just to employees.

- Vendors who collect personal information of students on behalf of school districts must be responsible for making sure that their children's data is available to parents upon request and correcting errors if challenged.

- In order to receive personal student information, vendors must have written contracts with education agencies or else all the specific requirements outlined in the law and the regulations for these contracts could be evaded. This is implied in the law and the regulations but it should be clearly stated.

- Education agencies should be required to post all contracts with vendors that receive personal student data or make them available within a limited period of time upon request, including which categories of personal student data the vendors are collecting and how parents may request access to that data. Education agencies should also have to explain why they are providing vendors access to this data and what is the educational purpose for this access.

- Breach notification to parents and affected parties should be carried out by snail mail and email; not phone calls, which are too difficult to verify and track.

- The regulations should incorporate all the powers and responsibilities of the Chief Privacy Officer as stated in Education Law §2-d; right now many are omitted from the proposed regulations, including the responsibility to issue an annual report on data breaches and improper data disclosures, as well as the results of investigations into parental complaints. This annual report should include information on how many districts are complying with the law, and providing the required training of staff in data privacy

and security. A deadline for the completion and release of this annual report should also be specified in the regulations.

More detailed comments are below.

§121.1 Definitions

p. 6; lines 54-55:

(o) *Student means any person attending or seeking to enroll in an educational agency*.

Add: "or a former student" who must also be covered under the law.

lines 56-57:

(p) *Student Data means personally identifiable information from the student records of an educational agenc*y.

Add: "or collected by vendor on behalf an educational agency."

§121.2 Educational Agency Data Collection Transparency and Restrictions.

p. 7 – important to add:

d*) No educational agency shall disclose personally identifiable information to any contractor or third party without a contract or written agreement that specifies its use and the conditions under which it will be kept private and secure.*

This is implied – that contracts or written agreements are required but never explicitly stated in the text of the regs.

Also need to add from Ed Law §2D but missing in the regs:

e) *Except as required by law or in the case of educational enrollment data, school districts shall not report to the department the following student data elements:(1) juvenile delinquency records;(2) criminal records;(3) medical and health records; and(4) student biometric information.*

§121.3 Parents Bill of Rights for Data Privacy and Security

p. 7, lines 92-93:

(a) Each educational agency shall publish on its website a parent's bill of rights for data privacy and security ("parent's bill of rights") that complies with the provisions of Education Law §2-d (3).

The above should include the State Education website which currently lacks any mention of four prominent and critical applicable federal student privacy laws, including PPRA, IDEA, COPPA and NSLA.

Lines 115-116:

(4) *if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected .*

The word "if" above should be deleted. According to FERPA, parents and eligible students have the right to challenge the accuracy of any of the personal data that pertains to them.

p. 9, line 121:

(6) address encryption of the data as provided in Education Law §2-d 5(f)(5).

The mode of encryption should be spelled out as it is on p. 14 - Section 121.9

Also add: These contracts shall be posted on the agency's website or be available upon request within 30 days.

And: For each contract, information should be included as to whether parents may opt out of the specific data disclosure and if so, how they may do so.

§121.5 Data Security and Privacy Standard.

p. 10, lines 153-155:

(a)As required by Education Law §2-d (5), the Department adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the standard for data security and privacy for educational agencies.

As NIST Framework is updated regularly in order to respond to new cybersecurity threats, the regulations should say that these requirements may themselves be updated regularly.

lines 163-164**:**

c (1) every use of personally identifiable information by the educational agency shall benefit students and the educational agency (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

The word "disclosure" should be added to the above; so that it reads "every use AND DISCLOSURE" of personally identifiable information.

p. 11 lines 169-172:

2*(d) An educational agency's data security and privacy policy shall include all the protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes.*

It is important to add the protections granted under federal laws PPRA, NSLA and COPPA here as well as include them in the Parent Bills of Rights..

Lines 173-174:

2 (e) *Each educational agency must publish its data security and privacy policy on its website and provide notice of the policy to all its officers and employees*.

Add: "and to all parents."

§121.6 Data Security and Privacy Plan.

Line 189:

4 *comply with Education Law §2-d.*

Add: "including the encryption requirements specified in Section 121.9 (6)

§121.9 Third Party Contractors

p. 13 lines 217-218

A 2) *limit access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services*

ADD: these sub-contractors shall be specified in the contract.

lines 221-223:

(4) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency, not disclose any personally identifiable information to any other party:

Question: how does this differ from (2) above?

lines 231-234

(5) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody as prescribed by state and federal law, regulations and its contract with the educational agency;

"Reasonable" has no substantive meaning here; it should instead say "industry best practices"

p. 14; lines 239-241:

(7) *not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.*

Add the word "license" after sell – i.e. "not sell or license PII"

§121.10 Reports and Notifications of Breach and Unauthorized Release

lines 258-259

(d) Educational agencies shall report every discovery or report of a breach or unauthorized release of student or teacher data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery .

This seems to repeat the same words as in (b) above, lines 253-253; see below:

(b) Each educational agency shall in turn notify the Chief Privacy Officer of 252 the breach or unauthorized release no more than 10 calendar days after it receives the 253 third-party contractor's notification in a format prescribed by the Department

p. 15, line 261:

(e) Educational agencies shall notify affected parents, eligible students, teachers and/or principals in the most expedient way possible ….

Add: former students should be informed to the degree possible if their PII has been breached

lines 275-281 etc.:

(*g) Notifications required by this section shall be clear, concise, use language 275 that is plain and easy to understand, and to the extent available, include: a brief 276 description of the breach or unauthorized release, the dates of the incident and the 277 date of discovery, if known; a description of the types of personally identifiable 278 information affected; an estimate of the number of records affected; a brief description 279 of the educational agency's investigation or plan to investigate; and contact information 280 for representatives who can assist parents or eligible students that have additional 281 questions .*

ADD: Notifications shall also include what actions affected individuals can take to mitigate the damage from the breach, as well as what actions the party responsible for the breach will take to mitigate the damage.

p. 16: lines 283-284:

(h) *Notification must be directly provided to the affected parent, eligible student, teacher or principal by first-class mail to their last known address; by email; or by telephone.*

Notification should occur by email AND first-class mail; not by telephone as there will be no record of the message and thus no proof of whether it occurred. Also former students should be notified as well if their PII is breached.

§121.12 Right of Parents and Eligible Students to Inspect and Review Students Education Records

lines 350-351:

(c) Requests by a parent or eligible student for access to a student's education records must be directed to an educational agency and not to a third-party contractor.

ADD: "and the educational agency shall arrange for the records to be delivered to the parent or eligible student."

d) *Educational agencies are required to notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by an educational agency.*

ADD: or any student data stored or maintained by a contractor on the agency's behalf.

§121.13 Chief Privacy Officer's Powers

pp. 19-20

There are many more powers and responsibilities enumerated of the CPO in Section 2D of the Education Law than those mentioned here. These should all be included here, including the responsibility to issue " *an annual report on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaints."*

This report for the previous school year should be released to the public and posted on the State Education Department website by Jan. 1 of each year, and made available upon request to any interested party. All of the following functions of the Chief Privacy Office included in Education Law §2-d should be incorporated into the regulations:

b. The functions of the chief privacy officer shall include, but not be limited to:

(1) promoting the implementation of sound information practices for privacy and security of student data or teacher or principal data;

(2) assisting the commissioner in handling instances of data breaches as well as assisting the commissioner in due process proceedings regarding any alleged breaches of student data or teacher or principal data;

(3) providing assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data or teacher or principal data;

(4) formulating a procedure within the department whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities the chief privacy officer determines is appropriate, may request information pertaining to student data or teacher or principal data in a timely and efficient manner;

(5) assisting the commissioner in establishing a protocol for the submission of complaints of possible breaches

of student data or teacher or principal data;

(6) making recommendations as needed regarding privacy and the security of student data on behalf of the department to the governor, the speaker of the assembly, the temporary president of the senate, and the chairs of the senate and assembly education committees; and

(7) issuing an annual report on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to subparagraph five of this paragraph.

c. The chief privacy officer shall have the power to:

(1) access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data;

(2) to review and comment upon any department program, proposal, grant, or contract that involves the processing of student data or teacher or principal data before the commissioner begins or awards the program, proposal, grant, or contract; and

(3) any other powers that the commissioner shall deem appropriate.

Submitted by the Parent Coalition for Student Privacy, NYS Allies for Public Education and Class Size Matters
For more information, please contact info@studentprivacymatters.org