





TO: P-12 Education Committee

FROM: Elizabeth R. Berlin 

SUBJECT: Proposed Addition of Part 121 to the Regulations of the Commissioner Relating to Student Data Privacy

DATE: January 3, 2019

AUTHORIZATION(S): 

SUMMARY

Issue for Discussion

Should the Board of Regents add a new Part 121 to the Commissioner's regulations to implement Education Law §2-d relating to protecting personally identifiable information?

Reason(s) for Consideration

Required by State statute - Education Law §2-d as enacted by Chapter 56 of the Laws of 2014.

Proposed Handling

The proposed amendment is presented to the P-12 Education Committee for discussion at the January 2019 Board of Regents meeting. A copy of the proposed amendment is included as Attachment A.

Procedural History

A Notice of Proposed Rule Making will be published in the State Register about January 30, 2019. Supporting materials are available upon request to the Secretary to the Board of Regents.

Background Information

Chapter 56 of the Laws of 2014 added §2-d to the Education Law effective April 2014. The focus of the law is the privacy and security of personally identifiable information (PII) of students, and certain annual professional performance review (APPR) data of teachers and principals. The law outlines certain requirements for educational agencies and their third-party contractors to ensure the security and privacy of such protected information.

Regulatory Background

The proposed amendments to Part 121 of the Commissioner's regulations were developed in consultation with stakeholders and the public. In 2017, the Chief Privacy Officer created the Data Privacy Advisory Council (DPAC) which consists of members drawn from diverse stakeholder groups and includes parents, industry advocates, administrative and teacher organizations and information technology experts. A list of DPAC members is included as Attachment B. The DPAC created two sub-committees to aid its work: the drafting workgroup and the technical standards workgroup. The drafting workgroup worked on the language of the regulation while the technical standards workgroup (drawn from a cross-section of experts from across the state) was responsible for recommending a standard for educational agency data security and privacy policies and practices. To seek public comments on additional elements of the parent's bill of rights and the regulation, the Department held fourteen public forums across the state in May and June and solicited for electronic comments during this period. The Chief Privacy Officer also created a Regulation Implementation Workgroup comprised of educational agency stakeholders from the field such as RIC Directors, BOCES staff, district technical directors and other experts in the field to collaborate in the work of developing an implementation roadmap, and other tools and resources to aid the adoption and implementation of the regulation and the data security and privacy standard it adopts. The input received from all stakeholders was critical to developing these regulations.

To highlight some provisions, Part 121 clarifies the data security and privacy obligations of educational agencies and third-party contractors; establishes requirements for contracts and other written agreements where PII will be provided to a third-party contractor and also attempts to clarify obligations where click-through agreements for software applications are utilized; establishes the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the standard for educational agencies data security and privacy programs; directs educational agencies to ensure that all employees that handle PII receive annual data security and privacy training; and requires that educational agencies identify a data protection officer that will be responsible for the educational agency's data security and privacy program.

Related Regents' Items

- [April 2018 Information Privacy Program Update](http://www.regents.nysed.gov/common/regents/files/518p12d1.pdf)
(<http://www.regents.nysed.gov/common/regents/files/518p12d1.pdf>)

Recommendation

Not applicable.

Timetable for Implementation

Following the 60-day public comment period required under the State Administrative Procedure Act, it is anticipated that the proposed rule will be presented to the Board of Regents for permanent adoption at its May 2019 meeting, and that the proposed amendment will become effective on July 1, 2019.

25 (f) Education Records means an education record as defined in the Family
26 Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g
27 and 34 C.F.R. Part 99, respectively.

28 (g) Educational Agency means a school district, board of cooperative
29 educational services (BOCES), school, or the Department.

30 (h) Eligible Student means a student who is eighteen years or older.

31 (i) FERPA means the Family Educational Rights and Privacy Act and its
32 implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

33 (j) NIST Cybersecurity Framework means the U.S. Department of Commerce
34 National Institute for Standards and Technology Framework for Improving Critical
35 Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel,
36 State Education Department, State Education Building, Room 148, 89 Washington
37 Avenue, Albany, New York 12234.

38 (k) Parent means a parent, legal guardian, or person in parental relation to a
39 student.

40 (l) Personally Identifiable Information, as applied to student data, means
41 personally identifiable information as defined in section 99.3 of Title 34 of the Code of
42 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20
43 U.S.C 1232-g, and as applied to teacher and principal data, means personally
44 identifying information as such term is defined in Education Law §3012-c(10).

45 (m) Release shall have the same meaning as Disclosure or Disclose.

46 (n) School means any public elementary or secondary school including a
47 charter school, universal pre-kindergarten program authorized pursuant to Education
48 Law §3602-e, an approved provider of preschool special education, any other publicly

49 funded pre-kindergarten program, a school serving children in a special act school
50 district as defined in Education Law §4001, an approved private school for the
51 education of students with disabilities, a State-supported school subject to the
52 provisions of Article 85 of the Education Law, or a State-operated school subject to the
53 provisions of Articles 87 or 88 of the Education Law .

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

56 (p) *Student Data* means personally identifiable information from the student
57 records of an educational agency.

58 (q) *Teacher or Principal Data* means personally identifiable information from
59 the records of an educational agency relating to the annual professional performance
60 reviews of classroom teachers or principals that is confidential and not subject to
61 release under the provisions of Education Law §§3012-c and 3012-d.

62 (r) *Third-Party Contractor* means any person or entity, other than an
63 educational agency, that receives student data or teacher or principal data from an
64 educational agency pursuant to a contract or other written agreement for purposes of
65 providing services to such educational agency, including but not limited to data
66 management or storage services, conducting studies for or on behalf of such
67 educational agency, or audit or evaluation of publicly funded programs. Such term shall
68 include an educational partnership organization that receives student and/or teacher or
69 principal data from a school district to carry out its responsibilities pursuant to Education
70 Law §211-e and is not an educational agency, and a not-for-profit corporation or other
71 nonprofit organization, other than an educational agency.

72 (s) Unauthorized Release means any release not permitted by federal or
73 State statute or regulation, any lawful contract or written agreement, or that does not
74 respond to a lawful order of a court or tribunal or other lawful order.

75

76

77 **§121.2 Educational Agency Data Collection Transparency and Restrictions.**

78 (a) Educational agencies shall not sell personally identifiable information nor
79 use or disclose it for any marketing or commercial purpose or facilitate its use or
80 disclosure by any other party for any marketing or commercial purpose or permit
81 another party to do so.

82 (b) Each educational agency shall take steps to minimize its collection,
83 processing and transmission of personally identifiable information.

84 (c) Each educational agency shall ensure that it has provisions in its contracts
85 with third party contractors or in separate data sharing and confidentiality agreements
86 that require the confidentiality of shared student data or teacher or principal data be
87 maintained in accordance with federal and state law and the educational agency's data
88 security and privacy policy.

89

90

91 **§121.3 Parents Bill of Rights for Data Privacy and Security.**

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

95 **(b) The parent’s bill of rights shall also be included with every contract an**
96 **educational agency enters with a third-party contractor that receives personally**
97 **identifiable information.**

98 **(c) Each educational agency shall include with its parent’s bill of rights**
99 **supplemental information for each contract the educational agency enters into with a**
100 **third-party contractor where the third-party contractor receives student data or teacher**
101 **or principal data. The supplemental information must be developed by the educational**
102 **agency and include the following information:**

103 **(1) the exclusive purposes for which the student data or teacher or principal**
104 **data will be used by the third-party contractor, as defined in the contract;**

105 **(2) how the third-party contractor will ensure that the subcontractors, or other**
106 **authorized persons or entities to whom the third-party contractor will disclose the**
107 **student data or teacher or principal data, if any, will abide by all applicable data**
108 **protection and security requirements, including but not limited to those outlined in**
109 **applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);**

110 **(3) the duration of the contract, including the contract’s expiration date and a**
111 **description of what will happen to the student data or teacher or principal data upon**
112 **expiration of the contract or other written agreement (e.g., if, when and in what format it**
113 **will be returned to the educational agency, and/or whether, when and how the data will**
114 **be destroyed).**

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

117 **(5) where the student data or teacher or principal data will be stored,**
118 **described in such a manner as to protect data security, and the security protections**

119 taken to ensure such data will be protected (e.g., offsite storage, using a cloud service
120 provider); and

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

122 (d) Each educational agency shall publish on its website the supplement to
123 the parent's bill of rights for any contract or other written agreement with a third-party
124 contractor that will receive personally identifiable information, provided that each such
125 supplement may be redacted to the extent necessary to safeguard the privacy and/or
126 security of the educational agency's data and/or technology infrastructure.

127

128

129 **§121.4 Parent Complaints of Breach or Unauthorized Release of Personally**

130 **Identifiable Information**

131 (a) Each educational agency must establish and communicate to parents and
132 eligible students its procedures for parents and eligible students to file complaints about
133 breaches or unauthorized releases of student data.

134 (b) The complaint procedures must require educational agencies to promptly
135 acknowledge receipt of complaints, commence an investigation, and take the necessary
136 precautions to protect any personally identifiable information.

137 (c) Following its investigation, the educational agency shall provide the parent
138 or eligible student with a report of its findings within a reasonable period but no more
139 than 30 calendar days from receipt of such complaint by the educational agency. In
140 extenuating circumstances, where the educational agency requires additional time to
141 investigate the complaint or cooperate with law enforcement, or where releasing the
142 report may compromise security or impede the investigation of the incident, the

143 educational agency shall provide the parent or eligible student with a written explanation
144 that includes the approximate date when the educational agency anticipates that the
145 report will be released.

146 (d) Educational agencies must maintain a record of all complaints of breaches
147 or unauthorized releases of student data and their disposition in accordance with
148 applicable data retention policies, including the Records Retention and Disposition
149 Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

150

151

152 **§121.5 Data Security and Privacy Standard.**

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

157 (b) No later than December 31, 2019, each educational agency shall adopt
158 and publish a data security and privacy policy that implements the requirements of this
159 Part and aligns with the NIST CSF.

160 (c) Each educational agency's data security and privacy policy must also
161 address the data privacy protections set forth in Education Law §2-d (5)(b)(1) and (2as
162 follows:

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

167 (2) personally identifiable information shall not be included in public reports or
168 other documents.

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

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

175

176

177 **§121.6 Data Security and Privacy Plan.**

178 (a) Each educational agency that enters into a contract with a third-
179 party contractor shall ensure that such contract includes a data security and
180 privacy plan. The data security and privacy plan must:

181 (1) outline how the third-party contractor will implement all state, federal, and
182 local data security and privacy contract requirements over the life of the contract,
183 consistent with the educational agency's data security and privacy policy;

184 (2) include a signed copy of the parent privacy bill of rights;

185 (3) include a requirement that any officers or employees of the third-party
186 contractor and its assignees who have access to student data or teacher or principal
187 data have received or will receive training on the federal and state law governing
188 confidentiality of such data prior to receiving access; and

189 (4) comply with Education Law §2-d.

190

191

192 **§121.7 Training for Educational Agency Employees.**

193 Educational agencies shall annually provide information privacy and security
194 awareness training to their officers and employees with access to personally identifiable
195 information. Such training may be delivered using online training tools and may be
196 included as part of training the educational agency already offers to its workforce.

197

198

199 **§121.8 Educational Agency Data Protection Officer**

200 Each educational agency shall designate one or more employees to serve as the
201 educational agency’s data protection officer(s) to be responsible for the implementation
202 of the policies and procedures required in Education Law §2-d and this Part, and to
203 serve as the point of contact for data security and privacy for the educational agency.
204 Such officer(s) must have the appropriate knowledge, training and experience to
205 administer the functions described in this part. This requirement may be fulfilled by a
206 current employee(s) of the educational agency who may perform this function in
207 addition to other job responsibilities.

208

209

210 **§121.9 Third Party Contractors**

211 (a) In addition to all other requirements for third-party contractors set forth in
212 this Part, each third-party contractor that will receive student data or teacher or principal
213 data shall:

- 214 (1) adopt technologies, safeguards and practices that align with the NIST
215 Cybersecurity Framework; comply with the data security and privacy policy of the
216 educational agency with whom it contracts; Education Law § 2-d; and this Part.
- 217 (2) limit access to personally identifiable information to only those employees
218 or sub-contractors that need access to provide the contracted services;
- 219 (3) not use the personally identifiable information for any purpose not
220 explicitly authorized in its contract;
- 221 (4) except for authorized representatives of the third-party contractor such as
222 a subcontractor or assignee to the extent they are carrying out the contract and in
223 compliance with state and federal law, regulations and its contract with the educational
224 agency, not disclose any personally identifiable information to any other party:
- 225 (i) without the prior written consent of the parent or eligible student; or
226 (ii) unless required by statute or court order and the third-party contractor
227 provides a notice of disclosure to the department, district board of education, or
228 institution that provided the information no later than the time the information is
229 disclosed, unless providing notice of disclosure is expressly prohibited by the statute or
230 court order.
- 231 (5) maintain reasonable administrative, technical and physical safeguards to
232 protect the security, confidentiality and integrity of personally identifiable information in
233 its custody as prescribed by state and federal law, regulations and its contract with the
234 educational agency;
- 235 (6) use encryption technology to protect data while in motion or in its custody
236 from unauthorized disclosure using controls as specified by the Secretary of the United

237 States Department of Health and Human Services in guidance issued under Section
238 13402(H)(2) of Public Law 111-5; and

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

242 (b) Where a third-party contractor engages a subcontractor to perform its
243 contractual obligations, the data protection obligations imposed on the third-party
244 contractor by state and federal law and contract shall apply to the subcontractor.

245

246

247 **§121.10 Reports and Notifications of Breach and Unauthorized Release**

248 (a) Third-party contractors shall promptly notify each educational agency with
249 which it has a contract of any breach or unauthorized release of personally identifiable
250 information in the most expedient way possible and without unreasonable delay but no
251 more than seven calendar days after such discovery of such breach.

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

255 (c) Third-party contractors must cooperate with educational agencies and law
256 enforcement to protect the integrity of investigations into the breach or unauthorized
257 release of personally identifiable information.

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

261 (e) Educational agencies shall notify affected parents, eligible students,
262 teachers and/or principals in the most expedient way possible and without unreasonable
263 delay, but no more than 14 calendar days after the discovery of a breach or
264 unauthorized release by an educational agency or the receipt of a notification of a
265 breach or unauthorized release from a third-party contractor unless that notification
266 would interfere with an ongoing investigation by law enforcement or cause further
267 disclosure of personal information by disclosing an unfixed security vulnerability. Where
268 notification is delayed under these circumstances, the educational agency shall notify
269 parents, eligible students, teachers and/or principals within seven calendar days after
270 the security vulnerability has been remedied or the risk of interference with the law
271 enforcement investigation ends.

272 (f) Where a breach or unauthorized release is attributed to a third-party
273 contractor, the third-party contractor shall pay for or promptly reimburse the educational
274 agency for the full cost of such notification.

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

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

286 (i) Upon the belief that a breach or unauthorized release constitutes criminal
287 conduct, the Chief Privacy Officer shall report such breach and unauthorized release to
288 law enforcement in the most expedient way possible and without unreasonable delay.

289

290

291 **§121.11 Third Party Contractor Civil Penalties**

292 (a) Each breach or unauthorized release of student data or teacher or
293 principal data by a third-party contractor shall be punishable by a civil penalty of the
294 greater of \$5,000 or up to \$10 per student, teacher, and principal whose data was
295 released, provided that the latter amount shall not exceed the maximum penalty
296 imposed under General Business Law §899-aa (6) (a).

297 (b) The Chief Privacy Officer shall investigate reports of breaches or
298 unauthorized releases of student data or teacher or principal data by third-party
299 contractors. As part of an investigation, the Chief Privacy Officer may require that the
300 parties submit documentation, provide testimony, and may involve visit to, or
301 examination and inspection of the third-party contractor's facilities and records by the
302 Chief Privacy Officer.

303 (c) Upon conclusion of an investigation, if the Chief Privacy Officer
304 determines that a third-party contractor has through its actions or omissions caused
305 student data or teacher or principal data to be breached or released to any person or
306 entity not authorized by law to receive such data in violation of applicable state or

307 federal law, the data and security policies of the educational agency, and/or any binding
308 contractual obligations, the Chief Privacy Officer shall notify the third-party contractor of
309 such finding and give the third-party contractor no more than 30 days to submit a written
310 response.

311 (d) If after reviewing the third-party contractor's written response, the Chief
312 Privacy Officer determines the incident to be a violation of the Education Law §2-d, the
313 Chief Privacy Officer shall be authorized to:

314 (1) order the third-party contractor be precluded from accessing personally
315 identifiable information from the affected educational agency for a fixed period of up to
316 five years; and/or

317 (2) order that a third-party contractor or assignee who knowingly or recklessly
318 allowed for the breach or unauthorized release of student data or teacher or principal
319 data be precluded from accessing student data or teacher or principal data from any
320 educational agency in the state for a fixed period of up to five years; and/or

321 (3) order that a third party contractor who knowingly or recklessly allowed for
322 the breach or unauthorized release of student data or teacher or principal data shall not
323 be deemed a responsible bidder or offeror on any contract with an educational agency
324 that involves the sharing of student data or teacher or principal data, as applicable for
325 purposes of the provisions of General Municipal Law §103 or State Finance Law
326 §163(10)(c), as applicable, for a fixed period of up to five years;

327 (4) require the third-party contractor to provide additional training governing
328 confidentiality of student data and/or teacher or principal data to all its officers and
329 employees with reasonable access to such data and certify that it has been performed,
330 at the contractor's expense. Such additional training must be performed immediately

331 and include a review of federal and state laws, rules, regulations, including Education
332 Law §2-d and this Part.

333 (e) If the Chief Privacy Officer determines that the breach or unauthorized
334 release of student data or teacher or principal data on the part of the third-party
335 contractor or assignee was inadvertent and done without intent, knowledge,
336 recklessness or gross negligence, the Commissioner may determine that no penalty be
337 issued upon the third-party contractor.

338

339

340 **§121.12 Right of Parents and Eligible Students to Inspect and Review Students**
341 **Education Records**

342 (a) Consistent with the obligations of the educational agency under FERPA,
343 parents and eligible students shall have the right to inspect and review a student's
344 education record by making a request directly to the educational agency in a manner
345 prescribed by the educational agency.

346 (b) An educational agency shall ensure that only authorized individuals gain
347 access to student data. To that end, educational agencies shall require identification or
348 verification of the identity of the parent or eligible student who requested access to an
349 education record.

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

353 (d) Educational agencies are required to notify parents annually of their right
354 to request to inspect and review their child's education record including any student

355 data stored or maintained by an educational agency. A notice issued by an educational
356 agency to comply with the FERPA annual notice requirement shall be deemed to satisfy
357 this requirement. Two separate annual notices shall not be required.

358 (e) Educational agencies shall comply with a request for access to records
359 within a reasonable period, but not more than 45 calendar days after receipt of a
360 request.

361 (f) Educational agencies may provide the records to a parent or eligible
362 student electronically, if the parent consents to such a delivery method. The educational
363 agency must transmit the personally identifiable information in a way that complies with
364 State and federal law and regulations. Safeguards associated with industry standards
365 and best practices, including but not limited to, encryption and password protection,
366 must be in place when education records requested by a parent or eligible student are
367 electronically transmitted.

368

369

370 **§121.13 Chief Privacy Officer's Powers**

371 The Chief Privacy Officer shall have the power to access all records, reports,
372 audits, reviews, documents, papers, recommendations, and other materials maintained
373 by an educational agency that relate to student data or teacher or principal data, which
374 shall include but not be limited to records related to any technology product or service
375 that will be utilized to store and/or process personally identifiable information. Based
376 upon a review of such records, the Chief Privacy Officer may require an educational
377 agency to act to ensure that personally identifiable information is protected in

378 accordance with state and federal law and regulations, including but not limited to
379 requiring an educational agency to perform a privacy and security risk assessment.

380

381

382 **§ 121.14 Severability.**

383 If any provision of this part or its application to any person or circumstances is
384 adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or
385 impair the validity of the other provisions of the article or their application to other
386 persons and circumstances, and those remaining provisions shall not be affected but
387 shall remain in full force and effect.

ATTACHMENT B

Data Privacy Advisory Council Membership <i>(as of 12/2018)</i>	
Heather Adams Assistant in Research and Educational Services New York State United Teachers	Tope Akinyemi Chief Privacy Officer New York State Education Department
Georgia Ascitto Executive Director Big 5	Joseph Baranello Chief Privacy Officer Office of the General Counsel New York City Department of Education
Kyle Belokopitsky Executive Director New York State Parent Teacher Association	Alison Bianchi General Counsel New York State Education Department
Kevin Casey Executive Director School Administrators Association of NYS	Charles Dedrick Executive Director New York State Council of School Superintendents
Jolene DiBrango Executive Vice President New York State United Teachers	Tracy Falvo Director of Technology Burnt Hills-Ballston Lake Central School District
Joseph E. Fitzgerald Assistant Director Lower Hudson Regional Information Center	David Gee Technology Director Fox Lane Middle School Bedford Central School District
Leonie Haimson Executive Director Class Size Matters	Beth Haroules Senior Staff Attorney New York Civil Liberties Union
Rose LeRoy Director of Educational Data and Research P12 Instructional Support New York State Education Department	Dr. Patrick McGrath Superintendent of Schools Burnt Hills-Ballston Lake Central School District
Lisa Rudley Steering Committee Member NYS Allies for Public Education	Julie Shaw, Esq. Partner Shaw, Perelson, May & Lambert
Colleen Sloan General Counsel Erie 1 BOCES	Amelia Vance Policy Counsel Future of Privacy Forum
Jay Worona General Counsel New York State School Board Association	

