







- (a) 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; or
- (b) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

**1. What kind of student data is *not* subject to the confidentiality and security requirements of Education Law §2-d?**

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de-identified data (e.g., data regarding students that uses random identifiers), aggregated data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student is not considered to be PII and is not within the purview of Education Law §2-d or within the scope of this Parents' Bill of Rights.

**2. What are my rights under Education Law § 2-d as a parent regarding my student's PII?**

Education Law §2-d ensures that, in addition to all of the protections and rights of parents under the federal FERPA law, certain rights will also be provided under the Education Law. These rights include, but are not limited to, the following elements:

- (A) A student's PII cannot be sold or released by the educational agency for any commercial or marketing purposes.
  - PII may be used for purposes of a contract that provides payment to a vendor for providing services to an educational agency as permitted by law.
  - However, sale of PII to a third party solely for commercial purposes or receipt of payment by an educational agency, or disclosure of PII that is not related to a service being provided to the educational agency, is strictly prohibited.
- (B) Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by an educational agency.
  - This right of inspection is consistent with the requirements of FERPA. In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.
  - NYSED will develop policies for annual notification by educational agencies to parents regarding the right to request student data. Such policies will specify a reasonable time for the educational agency to comply with such requests.

- The policies will also require security measures when providing student data to parents, to ensure that only authorized individuals receive such data. A parent may be asked for information or verifications reasonably necessary to ensure that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.

- (C) State and federal laws protect the confidentiality of PII, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

- (A) A mandate that, except as otherwise specifically authorized by law, NYSED shall only collect PII relating to an educational purpose;
- (B) NYSED may only require districts to submit PII, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under FERPA and/or the New York State Personal Privacy Law; and
- (C) Except as required by law or in the case of educational enrollment data, school districts shall not report to NYSED student data regarding juvenile delinquency records, criminal records, medical and health records or student biometric information.
- (D) Parents may access the NYSED Student Data Elements List, a complete list of all student data elements collected by NYSED, at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and
- (E) Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov). The complaint process is under development and will be established through regulations to be proposed by NYSED's Chief Privacy Officer, who has not yet been appointed.
  - Specifically, the Commissioner of Education, after consultation with the Chief Privacy Officer, will promulgate regulations establishing procedures for the submission of complaints from parents, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal APPR data by a third party contractor or its officers, employees or assignees.

- When appointed, the Chief Privacy Officer of NYSED will also provide a procedure within NYSED whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities may request information pertaining to student data or teacher or principal APPR data in a timely and efficient manner.

**1. Must additional elements be included in the Parents’ Bill of Rights.?**

Yes. For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents’ Bill of Rights each contract an educational agency enters into with a third party contractor shall include the following supplemental information:

- (A) the exclusive purposes for which the student data, or teacher or principal data, will be used;
- (B) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- (C) when the agreement with the third party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
- (D) 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; and
- (E) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
  - a. In addition, the Chief Privacy Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents’ Bill of Rights to be prescribed in Regulations of the Commissioner.

**2. What protections are required to be in place if an educational agency contracts with a third party contractor to provide services, and the contract requires the disclosure of PII to the third party contractor?**

Education Law §2-d provides very specific protections for contracts with “third party contractors”, defined as any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency. The term “third party contractor” also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an “educational agency.”

Services of a third party contractor covered under Education Law §2-d include, but not limited to, data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs.

When an educational agency enters into a contract with a third party contractor, under which the third party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy.

However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents' Bill of Rights must be included, as well as a requirement that any officers or employees of the third party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

Each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data shall:

- limit internal access to education records to those individuals that are determined to have legitimate educational interests
- not use the education records for any other purposes than those explicitly authorized in its contract;
- except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any PII to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the party provides a notice of the disclosure to NYSED, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
- maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and
- use encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

### **1. What steps can and must be taken in the event of a breach of confidentiality or security?**

Upon receipt of a complaint or other information indicating that a third party contractor may have improperly disclosed student data, or teacher or principal APPR data, NYSED's Chief Privacy Officer is authorized to investigate, visit, examine and inspect the third party contractor's facilities and records and obtain documentation from, or require the testimony of,

any party relating to the alleged improper disclosure of student data or teacher or principal APPR data.

Where there is a breach and unauthorized release of PII by a by a third party contractor or its assignees (e.g., a subcontractor): (i) the third party contractor must notify the educational agency of the breach in the most expedient way possible and without unreasonable delay; (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable delay; and (iii) the third party contractor may be subject to certain penalties including, but not limited to, a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.

## **1. Data Security and Privacy Standards**

Upon appointment, NYSED's Chief Privacy Officer will be required to develop, with input from experts, standards for educational agency data security and privacy policies. The Commissioner will then promulgate regulations implementing these data security and privacy standards.

## **2. No Private Right of Action**

Please note that Education Law §2-d explicitly states that it does not create a private right of action against NYSED or any other educational agency, such as a school, school district or BOCES.











