New York State Education Law §2-d
Third Party Contractor Requirements at a Glance

NYS Education Law §2-d has been in effect since April 2014. It applies to educational agencies and third party contractors, and is intended to limit collection and use of student data.

Who Must Comply?

The law applies to both educational agencies, including public schools, BOCES and NYSED) and third party contractors.

A third party contractor is any person or entity other than an educational agency, that receives student, teacher or principal data from an educational agency pursuant to a contract for purposes of providing services to the educational agency.

- Services include, but are not limited to data management or storage, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs.

What Data is Protected?

The law limits collection and use of student data, defined as personally identifiable information from student records of an educational agency. Personally identifiable information is defined in the same manner as in FERPA. The law also limits collection and use of personally identifiable information relating to the annual professional performance reviews of classroom principals or teachers.

Key Requirements for Third Party Contractors:

1. Personally identifiable information may not be sold or used for marketing purposes.

2. Each educational agency must publish a parents bill of rights for data privacy and security, which must be included in contracts with third party contractors.

   The parents bill of rights must state the following:
   a. A student's personally identifiable information cannot be sold or released for any commercial purposes;
   b. Parents have the right to inspect and review the complete contents of their child's education record;
   c. State and federal laws protect the confidentiality of personally identifiable information, 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**;
   d. A complete list of all student data elements collected by the State is available for public review at a website or a mailing address, to be included in the bill of rights and
   e. Parents have the right to have complaints about possible breaches of student data addressed. A phone number, email and mailing address must be included where parents can send complaints.

   The parents bill of rights must also include supplemental information for each contract an educational agency enters into with a third party contractor. The supplemental information must include:
   a. The exclusive purposes for which the student, teacher or principal data will be used;
   b. How the third party contractor will ensure that subcontractors, persons or entities with access to student, teacher or principal data with, if any, will abide by data protection and security requirements;
   c. When the agreement expires, and what happens to the student, 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, teacher or principal data will be stored and the applicable security protections, including whether the data will be encrypted.

Additional Contract Requirements:

Contracts must also include the following provisions and assurances by third party contractors:

1. That the confidentiality of the student, teacher or principal data will be maintained in accordance with federal and state law, and the educational agency's policy on data security and privacy
2. A data security and privacy plan outlining 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, including, but not limited to:
    a. Signed copy of the parents bill of rights for data privacy and security
    b. Requirement that any officers or employees of the third party contractor and its assignees who have access to student, teacher or principal data have received or will receive training on the federal and state law governing confidentiality of the data prior to receiving access
3. Access to education records will be limited to individuals with legitimate educational interests;
4. Education records will not be used except for purposes explicitly authorized in the contract;
5. Education records may only be shared with authorized representatives of the third party contractor to the extent they are carrying out the contract, and not to any other party without the prior written consent of the parent or eligible student; or unless required by statute or court order, with notice then provided to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless such notice is prohibited by the statute or court order;
6. The reasonable administrative, technical and physical safeguards maintained to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
7. Data will be encrypted in motion or in custody using a technology or methodology specified by the United States health and human services guidance issued under Section 13402(H)(2) of Public Law 111-5:
8. Requirement to notify the educational agency of any security breach resulting in an unauthorized release of data by the third party contractor or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of the educational agency and/or binding contractual obligations, in the most expedient way possible and without unreasonable delay.
    a. In the case of an unauthorized release of student, teacher or principal data, the educational agency shall notify the parent or eligible student, teacher or principal, respectively, of the unauthorized release of student data that includes personally identifiable information in the most expedient way possible and without unreasonable delay, and the third party contractor must promptly reimburse the educational agency for the full cost of such notification.

Enforcement Penalties:

Repercussions for violations include civil penalties of $5,000.00 or up to $10.00 per student, teacher, and principal whose data was released, whichever is larger, but not to exceed the maximum penalty under NY General Business Law §899-aa paragraph (a) of subdivision six.

If the NYS Chief Privacy Officer determines that the third party contractor or its assignee has violated applicable state or federal law, or the educational agency privacy and security policies by releasing student, teacher or principal data to an unauthorized person or entity, the third party contractor may also be:

1. Precluded from accessing student, teacher or principal data, as applicable, from the educational agency and/or from any educational agency in the state for up to five years;
2. Not deemed a responsible bidder or offerer on any contract with an educational agency that involves the sharing of student, teacher or principal data for up to five years; and/or
3. Required to provide training on federal and state law governing confidentiality of student, teacher or principal data to all its officers and employees with access to such data, prior to being permitted to receive subsequent access to such data

What's Next?

The chief privacy office, with input from parents and other education and expert stakeholders, is required to develop additional elements of the parents bill of rights for data privacy and security, and to develop standards for educational agency data security and privacy policies.

These policies will include:

1. Data privacy protections, including criteria for determining whether a proposed use of PII would benefit students and educational agencies, and processes to ensure that PII is not included in public reports or other public documents;
2. Data security protections, including data systems monitoring, data encryption, incident response plans, limitations on access to personally identifiable information, safeguards to ensure personally identifiable information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of personally identifiable information when no longer needed; and
3. Application of all such restrictions, requirements and safeguards to third-party contractors.