

New York State Education Department  
Education Law § 2-d

---

In the Matter of an Enforcement Action

against

**Order on Consent  
and  
Administrative Settlement**

**New York Therapy Placement Services, Inc.**  
(hereinafter referred to as "Respondent" )

---

1. The New York State Education Department ("Department") is charged with the general management and supervision of all public schools and all the education work of the State of New York from prekindergarten to graduate school, and is responsible for setting educational policy, standards, and rules. [Education Law § 101].
2. The Department, through its Commissioner and Chief Privacy Officer, is responsible for ensuring broad protections against the unauthorized release of student data pursuant to Education Law § 2-d and Part 121 of Title 8 of the Official Compilation of Codes, Rules and Regulations ("8 NYCRR"). The Department may investigate improper disclosures of student data and enforce violations against third-party contractors. [Education Law § 2-d[7][a]].
3. This Order is issued pursuant to the Department's authority under Education Law §§ 2-d, 101, 301, 305 (1) and 8 NYCRR Part 121.
4. Respondent New York Therapy Placement Services, Inc. is a for-profit New York corporation that is a third-party contractor or vendor offering special education services to New York educational agencies.
5. Respondent also has two locations included in the New York State Approved 4410 Preschool List, which is a list of special education preschool programs approved for State reimbursement.<sup>1</sup>
6. At least 125 educational agencies used Respondent's services on or before November 2023.
  - a. **Educational Agency** is defined in Education Law § 2-d(1)(c) as "school district, board of cooperative educational services (BOCES), school, or the education department." School is further defined to include
  - b. An approved provider of preschool special education;

---

<sup>1</sup> <https://www.nysed.gov/sites/default/files/programs/special-education/listings-of-new-york-state-approved-private-schools.xlsx>

7. **Student data** protected under Education Law § 2-d is defined in 8 NYCRR § 121.1(q) as “personally identifiable information (“PII”)<sup>2</sup> from the student records of an educational agency.”
- a. 8 NYCRR § 121.1(a) defines a **breach** as the “unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.”
  - b. 8 NYCRR § 121.1(e) defines **disclosure** to “mean to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.”
  - c. 8 NYCRR § 121.1(t) defines an **unauthorized disclosure or release** as “any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or [a disclosure] that does not respond to a lawful order of a court or tribunal or other lawful order.”
8. At the time of the Incident, Respondent’s Data Privacy and Security Plan dated September 29, 2023, provided that Respondent followed the “NIST Framework Version 1.1 to help manage its cybersecurity risk”<sup>3</sup> and listed its Nationwide Cybersecurity Review (NCSR) maturity level<sup>4</sup> for the majority of the five functions as a 6, which is tested and verified. The controls Risk Assessment (ID.RA), in the Identify function, Data Security (PR.DS) and Information Protection Processes and Procedures (PR.IP) in the Protect function were listed as a NCSR level 5, which is implementation in process. Finally, Awareness and Training in the Protect function is listed as NCSR level 4, which is partially documented standards and procedures.
9. The Data Privacy and Security Plan also provided that each employee receives data privacy training upon joining the company and that the employee manual, with which each employee must attest that they agree, contains sections on confidentiality and PII as in accordance with Federal, State, and local law, policy, and regulation including, without limitation, FERPA, NY Education Law Section 2-d, and [School] District policy.

### The Data Breach

10. On November 28, 2023, at approximately 11:30 AM, one of Respondent’s employees (“Compromised Employee”) received an email “that appeared to

---

<sup>2</sup> Personally Identifiable Information (“PII”) is defined in the Family Educational Rights Privacy Act (“FERPA”) [34 CFR §99.3] and is adopted in Education Law § 2-d and 8 NYCRR Part 121.

<sup>3</sup> Respondent’s Data Privacy and Security Plan is found by following the Data Privacy & Security Policy Link located on the footer of each page at <https://www.nytps.com/>.

<sup>4</sup> The NCSR Maturity Scale can be found at <https://www.cisecurity.org/ms-isac/services/ncsr>.

originate from [a client school] district that typically sends secure e-mails." Compromised Employee entered their Microsoft Office 365 ("Office 365") username and password in response to prompts provided in the email (the "data breach").

11. Within twenty-four hours, Compromised Employee's Office 365 email account had been used to send e-mails.
12. The data breach was discovered at approximately 1:18 PM on November 29, 2023.
13. According to Respondent, within 45 minutes of discovery, the Compromised Employee's network permissions and credentials were revoked. Compromised Employee received a new password for Office 365, as well as a new computer. Additionally, Compromised Employee's former computer was taken out of service and wiped clean.
14. During its investigation of the data breach, Respondent reviewed the contents of Compromised Employee's Office 365 OneDrive, where it discovered a "single report from 2021 which showed the names, addresses, and DOB of 41 children from 28 different districts."
15. On or about December 4, 2023, Respondent notified the 28 districts of the data incident and provided each with a list of its students whose PII was included in the 2021 report.

#### The Department's Review of Incident Reports from the Data Breach

16. After reviewing the incident reports filed by school districts that received data breach notifications from Respondent, the Department noted that Respondent did not disclose whether it reviewed the Compromised Employee's entire e-mail account (Inbox, Sent Items, Folders, Outbox, Junk, and Trash) or other Office 365 locations to which the Compromised Employee had access, such as SharePoint.
17. By letter dated December 20, 2023, the Department directed Respondent to "provide each affected school with a list of the students whose PII was included in email messages found in the [Compromised Employee's] email account (including inbox, mail folders, sent items, junk mail and trash), as well as the names of students whose PII was included in documents that the [Compromised Employee] could access from the employee's OneDrive account (including any SharePoint location or any other Microsoft Office 365 location that the [Compromised Employee] could access)."
18. The deadline for Respondent to provide the information was January 8, 2024.
19. Respondent responded on January 11, 2024, and stated that the Compromised Employee did not have access to any SharePoint sites and a review of their email

account concluded that the oldest email available in the account was dated January 19, 2016.

20. According to Respondent, on January 2, 2024, more than a month after the data breach occurred, it provided notice of the data breach to 134 entities, including 122 school districts, one BOCES, one § 4201 school, and one State-approved private (853) school. This notification stated that the type(s) of student data breached were student name, parent name, student home address, student home telephone number, and in some instances, student birth date.
21. Approximately 10 school districts reported receiving names of affected students from Respondent, who were not referred to Respondent for services.
22. On January 8, 2024, the Department asked Respondent for "the methodology used to determine how the school district notification lists were created" and a list of the entities that received the January 2, 2024, notification.
23. Respondent provided four possible reasons why a school district could have received names of students who the school district did not refer to Respondent, all of which were due to contact with Respondent that did not culminate in a referral from the school district for services.
24. The Department finds that Respondent's conduct violated Education Law § 2-d(5)(f)(4) and (6)(a), and 8 NYCRR Part 121.9(a)(1), (6), 121.10(a) which require third-party contractors that receive student data to maintain reasonable administrative, technical, and physical safeguards to protect PII, adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and notify educational agencies of a breach without unreasonable delay but no more than seven calendar days after the discovery of such breach.
25. Respondent acknowledges that it has been fully informed of the Department's position and hereby waives any right to a hearing as may be provided by law, consents to the issuance of this Order, and agrees to be bound by its terms. Respondent consents to and agrees not to contest the authority or jurisdiction of the Department to issue and enforce this Order and agrees not to contest the validity of this Order or its terms or the validity of reports submitted to the Department by educational agencies as a result of this breach.

**IT IS HEREBY ORDERED**, pursuant to the applicable provisions of the Education Law and 8 NYCRR Part 121:

26. The New York State Education Department assesses a civil penalty upon Respondent of \$125,000 for the violations(s) described above, however \$115,000 is suspended pending compliance with paragraphs 27 through 31 of this Order.

Respondent shall pay the remaining civil penalty of \$10,000 upon signing this Order.

27. Within ninety(90) days of the effective date of this Order, Respondent will provide evidence that all of its officers and employees with access to student data have received training on the federal and State laws and regulations governing confidentiality of student data This training must minimally encompass FERPA and New York State Education Law Section 2-d.
28. Within ninety (90) days of the effective date of this Order, Respondent will provide training, at its own expense, on cybersecurity fundamentals to all its officers and employees with access to Student data. This training shall minimally include phishing with a follow-up phishing exercise scheduled at least thirty (30) but not more than one hundred twenty (120) days after the initial training has been provided.
29. Within ninety (30) days of the effective date of this Order, Respondent will conduct a risk assessment to understand its' cybersecurity risk and shall procure insurance to cover the risk.
30. Respondent shall provide the Department with an affidavit attesting to the trainings and implementation completed in satisfaction of its obligations pursuant to Paragraphs 27 through 29 of this Order no later than April 17, 2024. The affidavit shall be sent to:

Chief Privacy Officer  
New York State Education Department  
89 Washington Avenue, Room 152  
Albany, New York 12234


31. Respondent shall submit this Order along with payment by mailing to:

Chief Privacy Officer  
New York State Education Department  
89 Washington Avenue, Room 152  
Albany, New York 12234

32. Upon completion of all obligations created in this Order, this Order settles only all claims for administrative penalties concerning the violations described above against Respondent and its successors and assigns.
33. The failure of Respondent to comply with any provisions in this Order shall constitute a default, shall be deemed to be a violation of both this Order and the Education Law and may subject Respondent to further penalties including preclusion from accessing student data from New York educational agencies.

- 34. No change in this Order shall be made or become effective except as set forth by a written Order of the Commissioner or the Chief Privacy Officer.
- 35. The effective date of this Order is the date that the Commissioner or the Chief Privacy Officer signs it.
- 36. This Order may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement, notwithstanding that all Parties are not signatories to the original or the same counterpart. For purposes of this order, copies of signatures shall be treated the same as originals. Documents executed, scanned, and transmitted electronically, and electronic signatures, shall be deemed original signatures for purposes of this Order and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

For Respondent:


  
 (signature of Respondent)  
Vice President  
 Title  
1/28/25  
 Date

On the 28th day of January in the year 2025, before me, the undersigned notary public, personally appeared Larry Johnston, personally known to me or proved to me on the basis of satisfactory evidence to be the individual(s) whose name(s) is (are) subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their capacity(ies), and that by his/her/their signature(s) on the instrument, the individual(s), or the person upon behalf of which the individual(s) acted, executed the instrument.

  
 Notary Public

Dated: Albany, New York, February 3, 2025

New York State Education Department

By:   
Louise DeCandia  
Chief Privacy Officer