NEW YORK THERAPY PLACEMENT SERVICES, INC.
DATA PRIVACY AND SECURITY PLAN
AND
EDUCATION LAW 2-d BILL OF RIGHTS FOR DATA PRIVACY & SECURITY
Updated: 02/25/2025

New York Therapy Placement Services, Inc. (NYTPS) values the trust placed in us by the school districts we serve. We are committed to safeguarding sensitive student data records in compliance with applicable federal and state regulations including New York State NYS Education Law §2-d and the *Family Educational Rights and Privacy Act* (FERPA).

To meet these obligations, NYTPS has implemented a cybersecurity and data protection program that aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and integrates best practices for securing sensitive information. Key aspects of our program include:

1. **Technical Safeguards**: Using encryption, network firewalls, and multi-factor authentication to ensure the confidentiality, integrity, and availability of sensitive data.
2. **Access Controls**: Restricting data access to authorized personnel with legitimate educational interests.
3. **Staff Training**: Educating employees on appropriate data privacy laws and cybersecurity practices.
4. **Incident Response**: Establishing clear protocols to promptly address and report data security incidents.
5. **Data Management**: Ensuring secure data storage, deletion, and transfer.

Our team works diligently to maintain compliance with all school district policies and the New York State Education Department's (NYSED) Parents' Bill of Rights. We are proud of our ongoing efforts to protect the privacy of students, teachers, and administrators.

ARTICLE ONE: PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

NYTPS has developed its Data Privacy and Security Plan to comply with applicable federal and state laws, including NYS Education Law §2-d and the Family Educational Rights and Privacy Act (FERPA). Our security plan incorporates the NIST Cybersecurity Framework, which guides our practices for protecting sensitive data. We adhere to school district policies and maintain an updated data security and privacy plan.

Outline the exclusive purposes for which student data will be used.

The student data received by NYTPS will be used only to perform its obligations pursuant to its agreements with the district and for no other purpose.

Outline how you will implement applicable data security and privacy contract requirements over the life of the contract.

NYTPS's compliance and IT personnel will coordinate to structure and implement data security and privacy practices pursuant to contractual obligations. NYTPS will periodically review its data security and privacy practices to ensure compliance with contractual obligations.

Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.

NYTPS follows applicable federal and state laws, including NYS Education Law §2-d and the Family Educational Rights and Privacy Act (FERPA). Our compliance program incorporates the NIST Cybersecurity Framework, which guides our practices for protecting sensitive data. We also adhere to school district policies and maintain an active data security and privacy plan.

NYTPS uses encryption technology to secure data both in transit and at rest. Our systems are protected by firewalls, multi-factor authentication, and access control measures to ensure only authorized personnel can access PII and/or student records. We conduct vulnerability assessments to strengthen our security posture.

Internal employees who have a need to access student records to perform their job duties are given password protected access to the data servers.

Field employees requiring access to electronic student records must be pre-authorized to access our network.

Both internal and field employees on the network are required to change their complex passwords every 90 days, and past passwords may not be repeated.

Address the training received by your employees, officers and any subcontractors engaged in the provision of services under the contract on the federal and state laws that govern the confidentiality of PII.

NYTPS employees, officers, and subcontractors are required to attend two training courses annually. These mandatory training courses are conducted by NYTPS. The first training course covers the specific data privacy and security requirements in New York State Education Law 2-d and FERPA. The second training course provides a general overview of cybersecurity, cybersecurity awareness, common types of cybersecurity attacks (phishing, spear phishing, ransomware, etc.), and ways to prevent cyber-attacks.

Additionally, NYTPS employees, officers, and subcontractors have access to publicly available data privacy and security policies of educational agencies with which NYTPS conducts business.

Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.

For employees, in addition to annual training courses that they must attend and sign an attestation that they have attended, each employee receives a copy of our employee manual which has detailed sections outlining the data privacy and security practices they must follow. This manual gets continually updated and redistributed as changes are made.

Contracts between NYTPS and the District may include provisions regarding the obligations of certain employees, agents, and subcontractors of the parties. NYTPS will incorporate relevant provisions and obligations into separate agreements with certain of its employees, agents, and subcontractors. NYTPS will also provide training for appropriate employees, agents, and subcontractors regarding the contractual obligations between it and the district.

Subcontractors who have access to PII to provide services to students are expected to maintain the same vigilance in protecting personally identifiable information as the Agency's employees. Independent contractors are required by written agreement to abide by materially similar confidentiality and data protection obligations imposed on NYTPS under state and federal laws and regulations, and the contract with the LEA. All independent contractors are required to complete NYTPS's online Data Privacy and Security Training upon engagement and periodically thereafter. This training reviews data protection and security requirements under state and federal laws governing confidentiality of student data, and the information contained in this Plan. All independent contractors must also sign the New York Therapy Placement Services, Inc. Business Associate Agreement and Corporate Compliance Plan which outlines the following responsibilities pertaining to safeguarding PII and/or PHI:

- PII will not be disclosed or discussed with others, including friends or family, who do not have a need to know it.
- PII will be used, disclosed, accessed, or viewed only to the extent required to carry out responsibilities, except as may be required by law.
- PII will not be discussed where others can overhear the conversation. It is not acceptable to discuss PII in public areas even if a patient's name is not used.
- Safeguards will be established to prevent unauthorized use, access, alteration, destruction, or disclosure of PII.
- Violations of any of the proceeding requirements will be immediately reported to New York Therapy Placement Services, Inc. at 631-473-4284.

- The provider is required to observe the same data protection, retention and destruction requirements as NYTPS with respect to student data and PII, as prescribed in contracts with educational agencies under which the provider delivers services, or as required by applicable law.

Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.

NYTPS uses administrative, technical, and physical safeguards to protect sensitive information. In the event of a data security incident, NYTPS maintains an Incident Response Plan ("IRP") to mitigate damage, investigate the cause, and recover services. This IRP is designed to:

- Provide guidelines for staff and service providers to respond to data security incidents.
- Reduce potential direct and indirect financial loss and other liability.
- Mitigate operational impact.
- Comply with regulatory requirements for information security under applicable law.
- Meet appropriate industry practices in accordance with the terms of our contractual obligations and applicable law.

NYTPS has appointed a qualified Incident Response Team (IRT) that is coordinated by the Information Security Officer to carry out the IRP. The IRP is based on National Infrastructure Protection Center (NIPC) guidelines, with additional regulatory reporting and notification requirements. Key guidelines are segmented into two phases:

Phase I: Detection, Assessment**,** Containment, Evidence Collection, Analysis and Investigation
Phase II: Remediation, Recovery, Post-Mortem, Notification

Phase I activities include the following:

1. Once an event is determined to be an Incident, use the *Incident Reporting Form* to begin documenting as much information about the Incident as possible.
2. Notify NYTPS ISO of the suspicious event.
3. Determine if an actual incident has occurred.
4. Protect evidence
5. Notify the appropriate internal and external personnel
6. Determine the incident severity level
7. Inform the Computer Data Security Management Committee
8. Evaluate response options
9. Notify external entities if the incident is found to reach beyond NYTPS-managed systems

Phase II Activities include the following:

1. Plan containment activities
2. Begin documenting incident response and recovery efforts
3. Execute containment activities and measure effectiveness of containment
4. Eradication (purge the affected systems and place back into its normal operating environment)
5. Recovery (if destruction or corruption of data has occurred)
6. Incident follow-up (understand root cause(s) of incident and evaluate strength of existing controls to defend against such incidents)

7. Document and File incident
8. Analyze evidence for criminal activity and notify appropriate law enforcement agencies
9. Develop and execute a communication plan to notify clients that may have been impacted by the event.
10. Finalize analysis and report
11. Archive evidence
12. Implement remediation
13. Analyze the Incident Response Team's incident response and make changes to the IRP if indicated.

Upon confirmation of a reportable incident, NYTPS will notify the educational agency of the incident without unreasonable delay and will comply with any individual educational agency's notification timeframe for breach notification, as specified in a contract with the educational agency.

NYTPS will assist the educational agency and/or law enforcement with their investigations into data security incidents reported by NYTPS.

Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations.

Please refer to Article Two below, specifically the section entitled Data Transition and Secure Destruction

Describe your secure destruction practices and how certification will be provided to the EA.

Please refer to Article Two below, specifically the section entitled Data Transition and Secure Destruction

Outline how your data security and privacy program/practices align with the EA's applicable policies.

New York Therapy is governed by the same data privacy laws as the EA. We have developed our data security and privacy practices to comply with NYS Education Law 2-d and FERPA. Further, we have built our cybersecurity management team and designed our security practices to follow the NIST CSF Version 2.

Outline how your data security and privacy program/practices materially align with the NIST CSF. Please include details regarding how you will identify, protect, respond to, and recover data security and privacy threats, as well as how you will manage your security controls.

NYTPS's internal cybersecurity management team includes a CISO with 30+ years' experience, Chief Operating Officer/Chief Compliance Officer, and IT Director. Additionally, we partner with external cybersecurity experts to assist us with identifying, containing, responding to, and reporting any security breaches to EAs and to the New York State Education Privacy Officer. These outside partners include forensic security firms, cyber insurance companies, and outside counsel with expertise in data privacy and cybersecurity. We also engage independent cybersecurity consultants to periodically audit our cybersecurity controls and are continually working to strengthen our security posture.

Please also refer to the preceding sections.

ARTICLE TWO: EDUCATION LAW 2-d BILL OF RIGHTS FOR DATA PRIVACY & SECURITY – SUPPLEMENTAL INFORMATION FOR CONTRACTS

Name of Contractor	New York Therapy Placement Services, Inc.
Description of the purpose(s) for which contractor will receive/access PII	To provide mandated related educational services.
Type of PII that contractor will receive/access	Student PII
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to data protection obligations imposed by state and federal laws and regulations. [ ] Contractor will not utilize subcontractors. [X] Contractor will utilize subcontractors.

This policy outlines the requirements for the retention and secure disposal of student data and PII held by NYTPS in compliance with New York State Education Law 2-d. This policy and the associated data retention schedule have been developed in accordance with the contracts between various educational agencies and NYTPS as a third-party contractor.

NYTPS' contracts cover multiple products, services, municipalities, districts, and schools. Accordingly, the terms of the contracts vary by product, service, municipality, district and/or school.

Data Retention & Destruction: NYTPS shall retain student data and PII only for the duration necessary to fulfill contractual obligations and/or as specified in the contract and during the contract term.

Secure Deletion: Upon the conclusion of the contract and/or the expiration of the retention period, NYTPS will securely delete and/or destroy all student data and PII using industry-accepted data destruction methods that prevent unauthorized access or reconstruction of the data.

Certificate of Destruction: NYTPS will maintain written certification of data destruction, including the types of data destroyed, method of destruction and date of destruction. Certificate(s) of destruction may be provided to an educational agency upon request.

Challenges to Data Accuracy:

A request from a parent or eligible student to amend, inspect, obtain copies of, or otherwise access student data must be received by NYTPS, or the LEA. NYTPS will assist the LEA in processing such requests in a timely manner, in accordance with procedure prescribed by the LEA. If a parent or eligible student feels the education record relating to the student held by NYTPS contains information that is inaccurate, misleading, or in violation of the student's privacy rights, he or she may submit a request to the LEA. If a correction to the information is deemed necessary by the LEA, NYTPS shall amend the records at the LEA's direction. NYTPS agrees to facilitate such corrections upon the written request of the LEA. If the

LEA decides not to amend the record as requested by the parent or eligible student, he or she will be notified by the LEA of the decision and of their right to a hearing regarding the request for amendment.

NYTPS will facilitate and comply with all requirements of the Parents' Bill of Rights under NYS Education Law 2-d, and that of the LEAs with which we conduct business, which can be found on the individual districts' websites.