

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -**SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	BIPTrack _____
PII Declaration	Does your organization/software collect student personally identifiable information (PII) or staff PII? Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
Description of the purpose(s) for which Contractor will receive/access PII	BIPTrack will hold PII related to student academic and therapy related data, including reports on said data. BIPTrack will also hold APPR PII related to staff names and their credentials for the purpose of enabling those staff members to collect data on approved students and produce reports.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☒ APPR PII



Contract Term	Contract Start Date <u>08/01/2023</u> Contract End Date <u>08/31/2024</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☒ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: All users access the BIPTrack portal via unique accounts, and any unauthorized access to user accounts is strictly prohibited. In the event of unauthorized access, the activity would be immediately reported to the affected agency, who would then be instructed to notify affected individuals as required by the major data security components of the HITECH Act. By default, access to PII is restricted. Each account's access to data and student information is controlled by administrative staff identified by Western Suffolk BOCES. This ensures the level of access to student information and specific BIPTrack features is appropriate for each user (such as staff, associates, and care-givers).
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Upon implementation, Western Suffolk BOCES staff roles will be identified and assigned. These roles define the type of PII and BIPTrack feature access each staff role type has by default. This access is then adjusted per user as appropriate for each PII. Roles include parents/care-givers, student supervisors, primary and secondary.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative and operational access to individual PII is restricted by default and is measured-out by Western Suffolk BOCES as appropriate for each user need to access said PII. All at-rest and in-motion data is encrypted. Access to PII by Western Suffolk BOCES users is restricted by default and can be adjusted up
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Officers and support staff at BIPTrack have received training on the federal and state laws governing confidentiality of protected data. Ongoing management oversight and quality assurance is maintained for monitoring compliance with the privacy and security safeguards regarding PII. Security practices are audited and adjusted as needed each quarter to conform to regulations.
4	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.	as required by HIPAA Security Final Rule (CFR 164.308(a)(1)). All safeguards and security protocols remain in full effect during recovery and emergency operations, as per HIPAA Security Final Rule (CFR 164.308(7)(ii) ©). Officers and support staff at BIPTrack have received training on the federal and state laws governing confidentiality of protected data. Ongoing management oversight and quality
5	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.	All users access the BIPTrack portal via unique accounts, and any unauthorized access to user accounts is strictly prohibited. All user access (including unique IP address and location) is logged for forensic and support purposes. In the event of unauthorized access, the activity would be promptly reported to the affected agency, who would then be instructed to notify affected individuals as required by the major data security components of the HITECH Act. A breach of PII includes the acquisition, access, use, or disclosure of PII in a manner not permitted by this Agreement which compromises the security or privacy of the PII.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	If/when requested, all or selected PII can be delivered as a database structure. Identified EA administrators have the ability to export notes/reports generated within BIPTrack for each student for any date range required. The BIPTrack API can also be used by authorized EA individuals to pull data from BIPTrack into
7	Describe your secure destruction practices and how certification will be provided to the EA.	EA-identified electronic PII is removed from the EA's BIPTrack database upon request as per Section 13402(h) of Title XIII HITECH Act. If EA PII data remains in BIPTrack, data backups created prior to the data removal will be securely deleted both on and off-site, rendering recovery of said data impossible. A detailed
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	All User activity is logged along with user IP address and location. All PII and APPR PII at-rest data is held in a HIPAA-compliant encrypted database container as required by Title XIII HITECH Act (Section 13402(h)). All end-to-end device communications (data transmission) are protected by an AES 256 bit
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	BIPTrack maintains an active response plan that incorporates the five core functions of NIST CSF v1.1: Identify, Protect, Detect, Respond, and Recover. This plan includes well-defined communication lines among appropriate parties, the collection and analysis of information

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	David KNight
[Title]	Chief Experience Officer
Date:	05/26/2023

January 13, 2022



PDFfiller Document ID: 3FC0-4C63-0360-0000