

**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).

<b>Name of Contractor</b>	Clinical Staffing Resources, Corp <hr/>
<b>PII Declaration</b>	<p><b>Does your organization/software collect student personally identifiable information (PII) or staff PII?</b></p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> <li>a. The student’s name;</li> <li>b. The name of the student’s parent or other family members;</li> <li>c. The address of the student or student’s family;</li> <li>d. A personal identifier, such as the student’s social security number, student number, or biometric record;</li> <li>e. Other indirect identifiers, such as the student’s date of birth, place of birth, and Mother’s Maiden Name;</li> </ul> <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> <li>a. Teacher Id, Social Security Number, Employee Number, Biometric Record</li> <li>b. Name, Mother's Maiden Name, Parent's Name</li> <li>c. Birthdate, Place of Birth, Address</li> <li>d. Gender, Race, Salary</li> </ul> <p><input type="checkbox"/> <b>IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</b></p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	We utilize this information for care required for students
<b>Type of PII that Contractor will receive/access</b>	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR PII</p>

<b>Contract Term</b>	Contract Start Date <u>07/01/2024</u> Contract End Date <u>06/30/2025</u>
<b>Subcontractor Written Agreement Requirement</b>	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)  <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	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.
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)  <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other:  Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

**CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN**

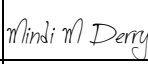
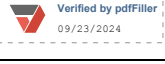
The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a 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.	Please see attached Data Privacy policy
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please see attached Data Privacy policy
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.	Please see attached Data Privacy policy
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.	Please see attached Data Privacy policy
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.	Please see attached Data Privacy policy
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please see attached Data Privacy policy
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please see attached Data Privacy policy
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please see attached Data Privacy policy
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please see attached Data Privacy policy

# 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](http://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](mailto:dpo@wsboces.org). (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://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](mailto: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]	Mindi M Derry
[Title]	VP
Date:	03/12/2024



## DATA PRIVACY AND SECURITY POLICY

### I. Purpose

This policy addresses Clinical Staffing Resources (“Agency”) responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources. The Agency takes active steps to protect the confidentiality of protected information in compliance with all applicable state and federal laws. The Agency likewise expected all Agency officers, employees, and partners to maintain the confidentiality of protected information in accordance with state and federal law and applicable Agency policies.

### II. Policy

Statement It is the responsibility of the Agency:

- (1) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information.
- (2) to maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the Department of Education’s mission.
- (3) to protect, and not sell or disclose for marketing or commercial purposes, personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure.
- (4) to address and require the adherence of its vendors with federal, state and SED requirements in its vendor agreements, especially 8 NYCRR Part 121.
- (5) to train its users to share a measure of responsibility for protecting SED’s data and data systems.
- (6) to identify its required data security and privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and
- (7) to communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

### III. Standard

The Agency will use the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

### IV Scope

The policy applies to Agency officers, administrators, and employees, and also to independent/subcontractors, interns, volunteers ("Users") and third-party contractors who receive or have access to the Agency's data and/or data systems. This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of the Agency and it addresses all information, regardless of the form or format, which is created or used in support of the activities of an educational agency. This policy, as implemented, shall ensure that every use and disclosure of personally identifiable information by the Agency shall benefit students and the Agency and shall ensure that personally identifiable information shall not be included in public reports or other documents. This policy shall be published on the Agency website and notice of its existence shall be provided to all employees and Users.

### V. Compliance

All Users are responsible for the compliance of their programs with this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and Users will be directed to adopt corrective practices, as applicable.

### VI. Oversight

The Agency shall appoint a Data Protection Officer who shall annually report to the VP on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to Education Law §2-d. The Data Protection Officer will also be responsible for the implementation of the policies and procedures required in Education Law § 2-d and its implementing regulations, and will serve as the point of contact for data security and privacy for the Agency.

### VII. Data Privacy

(1) Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2- d and other state or federal laws addressing data security and confidentiality shall be adhered to at all times.

(2) Data protected by law must only be used in accordance with law and regulation and the Agency policies to ensure it is protected from unauthorized use and/or disclosure.

(3) The Agency has established a Data Protection Officer and a Data Privacy Committee to manage its use of data protected by law. The Data Protection Officer and the Data Privacy Committee will determine whether a proposed use of personally identifiable information would benefit students and educational agencies, and to ensure that personally identifiable

information is not included in public reports or other public documents, or otherwise publicly disclosed.

(4) No student data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulations.

(5) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with Agency procedures.

(6) It is the Agency's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, the Agency shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.

(7) Contracts with third parties that will receive or have access to personally identifiable information must include a Data Privacy and Security Plan that outlines how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

#### VIII. Right to Inspect

Parents and eligible students shall have the right to inspect and review a student's education record by making a request directly to the Agency in writing. Only authorized individuals shall be able to inspect and review student data, and the Agency shall take all necessary measures to verify the identity of parents and eligible students, and his/her authority to do so, who submit requests to inspect and review an educational record. The Agency shall comply with a request for access to records within a reasonable period of time, but not more than 45 calendar days after receipt of the request. The Agency shall transmit the personally identifiable information in a way that complies with state and federal law and regulations. Safeguards associated with industry standards and best practices shall be in place if and when education records requested by a parent or eligible student are electronically transmitted.

#### IX. Incident Response and Notification

The Agency will respond to data privacy and security critical incidents or allegations of breach of data in accordance with Education Law §2-d and Commissioner's regulations Part 121. All breaches of data and/or data systems must be reported to the Data Protection Officer. All breaches of personally identifiable information or sensitive/confidential data must be reported to the Data Protection Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal personally identifiable information as defined by Education law §2-d, or any Agency sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data. State and federal laws require that affected individuals must be notified when

there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, the Superintendent, Data Protection Officer, school attorneys, and other subject matter experts will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay. Parents, eligible students, teachers, principals or other staff of the Agency may file a written complaint about breaches or unauthorized releases of student data and/or teacher or principal data. The complaint must be filed with the Agency in writing. Upon receiving such a complaint, the Agency will promptly acknowledge receipt of same, commence an investigation, and take any necessary precautions to protect personally identifiable information. Following its investigation, the Agency shall provide the complainant with its findings no more than 60 calendar days from the date the Agency received the complaint. Should the Agency require additional time to relay its findings, or where the response may compromise security or impede a law enforcement investigation, the Agency shall provide the complainant with a written explanation that includes the approximate date when the Agency anticipates that it will respond to the complaint. A record of all complaints of breaches or unauthorized releases of student data shall be maintained by the Agency in accordance with applicable data retention policies.

X. Acceptable Use Policy, Password Policy and other Related Agency Policies

(1) Users must comply with the Acceptable Use Policy in using the Agency's resources. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with the Agency's missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the Agency or moved to another position.

(2) Users must comply with all other related Agency policies.

XI. Training

All users of the Agency's data, data systems and data assets must annually complete the information security and privacy training offered by the Agency. Information security and privacy training will be made available to all users. Employees must complete the training annually, and such training may be delivered using online training tools and be included as part of professional development training.