

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).

| | |
|--|--|
| <p>Name of Contractor</p> | <p>H.E.A.R.S. Audiology, P.C.</p> <hr/> |
| <p>PII Declaration</p> | <p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> 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; <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> <p>If you collect the PII information above, please complete the remainder of this form.</p> |
| <p>Description of the purpose(s) for which Contractor will receive/access PII</p> | <p>To complete Hearing and Auditory Processing Evaluation histories with accurate information. Protected Data shall not be used for any other purposes than those explicitly authorized by contract with educational agency.</p> |
| <p>Type of PII that Contractor will receive/access</p> | <p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR PII</p> |

| | |
|--|--|
| Contract Term | Contract Start Date <u>07/01/2022</u> Contract End Date <u>07/01/2023</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) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors. |
| Data Transition and Secure Destruction | Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • 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) <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 checked="" type="checkbox"/> Other: All hard copy notes and documents will be stored in a locked secured cabinet/file room located at 732 Smithtown Bypass, Smithtown, NY. The cabinet/file room key is also kept in a locked closet inside the office, which is locked at all times when the office is unoccupied. Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: State, federal, and local data security and privacy contract requirements will be implemented by utilizing best practices and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, and limitations of access to stored data to authorized staff. H.F.A.R.S. Audiology, P.C. keeps softwares updated and utilizes multi-factor authentication to mitigate vulnerability of cyber security. |
| 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. | All networks are secured by a high rated firewall and intrusion detection/prevention system. All computers are password protected with time out settings activated. In the event that it becomes necessary to transmit confidential data through email, encryption technology shall be used to protect data from unauthorized disclosure. |
| 2 | Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII. | Student information and data are kept out of view when other patients, contractors, service providers, or non-employees are present. Documents in progress are never left in full view on the computer monitor when unoccupied and all time-out settings for all computers are set conservatively. |
| 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. | All employees receive HIPAA training during the onboarding process. Additionally, all persons are informed of and consent to following the data security and privacy plan. |
| 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. | Persons or entities with which H.E.A.R.S. Audiology, P.C. will share Protected Data, if any, will abide by the requirements of our data security and privacy plan, and any contractual obligations with respect to Protected Data set forth in agreement with the disclosing party. All employees or other personnel are required to sign a written confidentiality agreement. |
| 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. | The current data security and privacy plan will be monitored and upgraded to meet an/or exceed industry standards. Any incident will be immediately documented, repaired, and reported to the EA by H.E.A.R.S. Audiology, P.C. |
| 6 | Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. | When no longer necessary, all data will be transitioned to the EA via secure carrier, whether certified mail, FedEx, etc. |
| 7 | Describe your secure destruction practices and how certification will be provided to the EA. | H.E.A.R.S. Audiology, P.C. utilizes a secure shredding service which ensures protection and destruction of confidential information safely while complying with regulations and privacy laws. The EA will be provided with a Certification of Destruction to confirm material has been securely destroyed. |
| 8 | Outline how your data security and privacy program/practices align with the EA's applicable policies. | Our employees receive relevant data security and privacy information and are required to sign a HIPAA and confidentiality agreement. We will have sufficient internal controls including but not limited to encryption, firewalls, and password protection. |
| 9 | Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 | All networks at our practice are secured by a high rated firewall and intrusion detection/prevention system. In case of detection of a cybersecurity event, incident will be documented, repaired, and reported to the EA. |

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] | <i>Kathleen Page</i> |
| [Printed Name] | Kathleen Page |
| [Title] | Audiologist & Practice Owner |
| Date: | 06/27/2022 |

January 13, 2022



PDFfiller Document ID: 0487-3DE7-B86E-0005