DATA PRIVACY AGREEMENT

INCLUDING PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY AND SUPPLEMENTAL INFORMATION ABOUT THE AGREEMENT

1. **Purpose**

- (a) This Data Privacy Agreement (DPA) supplements the agreement between Watervliet City Schools (THE DISTRICT) and Healthy Alliance IPA, LLC (Vendor), to ensure that the Vendor AGREEMENT conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Agreement consists of the terms of this DPA Agreement, a copy of Watervliet City School District Parents Bill of Rights for Data Security and Privacy signed by Vendor and the Supplemental Information about the AGREEMENT that is required to be posted on district's website.
- (b) To the extent that any terms contained within the Vendor AGREEMENT, or any terms contained within any other Agreements attached to and made a part of the Vendor AGREEMENT, conflict with the terms of this DPA, the terms of this DPA will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the Vendor AGREEMENT, to the extent that any term of the TOS conflicts with the terms of this DPA, the terms of this DPA will apply and be given effect.

2. **Definitions**

Any capitalized term used within this DPA that is also found in the Vendor AGREEMENT will have the same definition as contained within this DPA.

In addition, as used in this Exhibit:

- (a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from the district pursuant to the DPA.
- (b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from the district pursuant to the Vendor AGREEMENT.
 - (c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the AGREEMENT may originate from the district located across New York State, and that this Protected Data belongs to and is owned by the district from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and THE DISTRICT policy on data security and privacy. Vendor acknowledges that THE DISTRICT is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to Vendor.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from the district in accordance with the district's Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by Vendor and is set forth below.

Additional elements of Vendor' Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this DPA, consistent with THE DISTRICT data security and privacy policy, Vendor will: [Maintain existing processes and policies in place for regulatory compliance with HIPAA, 42 CFR Part 2, NYS Mental Hygiene Law, Article 27-F of PSL, and FERPA. Vendor will maintain existing Data Lots Prevention safeguards for ePHI and PII. Vendor will maintain Email filtration, vulnerability remediation, and security awareness training programs.
- (b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Vendor AGREEMENT, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Vendor AGREEMENT:

Internal/External penetration testing, Phish Testing, Risk Assessment, Monthly Vulnerability Assessments and	Role-Based
Security Awareness Training.	1

(c)	Vendor will	comply wi	th all	obligations	set forth	in	THE	DIST	RICT	
"Suppl	emental									
Information a	bout the AGI	REEMENT"	belov	V.						

(d)	For any	of its of	ficers or	employees	(or	officers	or e	nployees	of any	of its
subcontractors o	r assigne	ees) who	have ac	cess to Pro	tecte	d Data,	Vendo	or has pr	ovided c	or will
provide training	on the fe	deral and	l state lav	ws governin	g con	fidential	ity of	such data	a prior to	o their
receiving access,	as follow:	s:								
r Data Security and Pr	ivacy Aware	noce Trainir	a required	to be complete	d annu	بالد				

Data Security and Privacy Awareness Training required to be completed annually.

- (e) Vendor [check one] ____will _X _will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Vendor AGREEMENT. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Vendor AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in THE DISTRICT "Supplemental Information about the Vendor AGREEMENT," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in THE DISTRICT "Supplemental Information about the AGREEMENT," below.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from the district, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Vendor AGREEMENT and the terms of this Data Privacy Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the Vendor AGREEMENT.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
 - (d) Not disclose any personally identifiable information to any other party, except for

authorized representatives of Vendor using the information to carry out Vendor's obligations under the Vendor AGREEMENT, unless:

- (i) the parent or eligible student has provided prior written consent; or
- (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the district no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in THE DISTRICT "Supplemental Information about the Vendor AGREEMENT," below.
- (g) Provide notification to THE DISTRICT (to the extent required by, and in accordance with, Section 6 of this Data Privacy Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse THE DISTRICT, for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

- (a) Vendor shall promptly notify THE DISTRICT of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.
- (b) Vendor will provide such notification to THE DISTRICT by contacting THE DISTRICT: Data Protection Officer or Designee
- (c) Vendor will cooperate with THE DISTRICT and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the district affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

- (d) Vendor acknowledges that upon initial notification from Vendor, THE DISTRICT, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by THE DISTRICT, Vendor will promptly inform the Data Protection Officer or designees.
- (e) Vendor will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to the DISTRICT or Regional Information Center.

BY	Vo	nd	Λr	
DІ	VC	ш	W	

Erica Coletti	Frica Coletti
Signature	
СЕО	
Title 2021-11-30	
Date	
Tom McCarrell	Tom McCarroll

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

The Watervliet City School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- 2) Parents have the right to inspect and review the complete contents of their child's education record.
- 3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- 4) A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/student-data-privacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents/guardians who believe there has been a possible breach of student data should direct their concerns/complaints to the District Data Protection Officer, Kirsten DeMento at 518-629-3231 or kdemento@vlietschools.org.
- 6) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Watervliet City School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

- 3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6. Address how the data will be protected using encryption while in motion and at rest.
- 7. Third-party contractors are also required to:
 - a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student date or teacher or principal data;
 - b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
 - c. Not use educational records for any other purpose than those explicitly authorized in the contract;
 - d. Not disclose personally identifiable information to any other party without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
 - e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
 - f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law 2-d;
 - g. Notify Watervliet City School District of any breach of security resulting in an unauthorized release of student data, in the most expedient way possible and without unreasonable delay;
 - h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
 - i. Provide a signed copy of this Bill of Rights to the Watervliet City School District thereby acknowledging that they aware of and agree to abide by this Bill of Rights.
- 8) This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department Chief Privacy Officer, as well as emerging guidance documents.

BY Vendor:	
Erica Coletti	Erica_Colett
Signature	
CEO	
Title	
2021-11-30	
Date	

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN WATERVLIET CITY SCHOOLS AND Vendor

Watervliet City Schools has entered into An Agreement ("AGREEMENT") with Vendor ("Vendor"), which governs the availability to the district of the following Product(s):

Pursuant to the AGREEMENT, the district may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: To improve health and lower the total cost of care for vulnerable individuals through a focus on Social Determinants of Health referral data on the Service Software.

Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors:In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the AGREEMENT and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: [Describe steps the Vendor will take]

Duration of AGREEMENT and Protected Data Upon Expiration:

- The AGREEMENT commences on [the date the district's BOE accepts the agreement) and expires on [a date that is mutually agreed on in the future]. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors. If requested by the district, the Vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At THE DISTRICT request, Vendor will cooperate with THE DISTRICT as necessary in order to transition

Protected Data to any successor Vendor prior to deletion.

Vendor agrees that neither it nor its subcontractors, assignees, or other authorized agents will
retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on
any storage medium whatsoever. Upon request, Vendor and/or its subcontractors, assignees, or
other authorized agents will provide a certification from an appropriate officer that these
requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the district to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights

and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

By vendor:	
Erica Coletti	Erica Co lett
Signature	
CEO	
Title	
2021-11-30	
Date	

Signature Certificate

Document name:

Watervliet City School District - Healthy Alliance IPA - Data Use Agreement (DUA)

Unique Document Id:

50ac04fb-f682-42f2-91a1-1e74d4010794

Document fingerprint:

cc7e1b11b6e82146aefc5e47941b77b8b67ae0b4adfe8c1e26997ed962a3de1d8bbdab9a28b62a1f17f732b75f82b224f2662ae1d9b5797f72b94b2b67d56080

Signatories



Erica Coletti

EO

Alliance for Better Health Care, LLC / Healthy Alliance IPA LLC

Email: erica.coletti@abhealth.us

Device: Mobile Safari 14.1 on iOS 14.8 AP iPhone (smartphone)

IP number: 67.246.41.122

IP Location: Ballston Spa, New York, United States

Trusted timestamp: 2021-11-30 18:40:51 UTC

Erica Coletti

This document was completed by all parties on:

2021-11-30 18:40:51 UTC



Audit log

Trusted timestamp	Event with collected audit data
2021-11-30 18:40:51 UTC	Document was signed by Erica Coletti (erica.coletti@abhealth.us) Device: Mobile Safari 14.1 on iOS 14.8 AP iPhone (smartphone) IP number: 67.246.41.122 - IP Location: Ballston Spa, New York, United States
2021-11-30 18:40:47 UTC	Document was verified via handwritten signature by Erica Coletti (erica.coletti@abhealth.us) Device: Mobile Safari 14.1 on iOS 14.8 AP iPhone (smartphone) IP number: 67.246.41.122 - IP Location: Ballston Spa, New York, United States
2021-11-30 18:40:43 UTC	Document was reviewed by Erica Coletti (erica.coletti@abhealth.us) Device: Mobile Safari 14.1 on iOS 14.8 AP iPhone (smartphone) IP number: 67.246.41.122 - IP Location: Ballston Spa, New York, United States
2021-11-30 18:32:46 UTC	Document was opened by Erica Coletti (erica.coletti@abhealth.us) Device: Mobile Safari 14.1 on iOS 14.8 AP iPhone (smartphone) IP number: 67.246.41.122 - IP Location: Ballston Spa, New York, United States
2021-11-30 17:06:36 UTC	Document was sent to Erica Coletti (erica.coletti@abhealth.us) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-11-30 17:06:35 UTC	Document was sealed by Tom McCarroll (tom.mccarroll@abhealth.us) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-11-30 14:43:49 UTC	Document was created by Alliance for Better Health Contracting (philip.cassidy@abhealth.us) IP number: 35.171.45.60 - IP Location: Ashburn, Virginia, United States



Signature Certificate

Document name:

Watervliet City School District - Healthy Alliance IPA - Data Use Agreement (DUA)

Unique document ld: 8637dfad-58ea-4b26-9735-c631b812ac69

Document fingerprint:

9897a581b9c464b00bc11ef8d8bdf0b513d45337a3f0ade1bcbbaf7afc84afe4777b87f7f72979e41055b 7e89a4a887e5487f99f91eb1b223efcfb0c9f13086d

Signatories



Tom McCarroll

Vice-President Compliance and Privacy

Email: tommccarrollchc@gmail.com

Device: Chrome 96.0 on Windows 10 (desktop)

IP number: 45.47.160.59

IP Location: Delmar, New York, United States

Trusted timestamp: 2021-12-02 17:32:35 UTC

Tom McCarroll

This document was completed by all parties on:

2021-12-02 17:32:35 UTC



Audit log

Trusted timestamp	Event with collected audit data
2021-12-02 17:32:35 UTC	Document was signed by Tom McCarroll (tommccarrollchc@gmail.com) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-12-02 17:32:30 UTC	Document was verified via handwritten signature by Tom McCarroll (tommccarrollchc@gmail.com) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-12-02 17:32:23 UTC	Document was reviewed by Tom McCarroll (tommccarrollchc@gmail.com) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-12-02 17:31:59 UTC	Document was opened by Tom McCarroll (tommccarrollchc@gmail.com) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-12-02 17:16:16 UTC	Document was sent to Tom McCarroll (tommccarrollchc@gmail.com) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-12-02 17:16:15 UTC	Document was sealed by Alliance for Better Health Contracting (philip.cassidy@abhealth.us) Device: Chrome 96.0 on Windows 10 (computer) IP number: 45.47.160.59 - IP Location: Delmar, New York, United States
2021-12-02 15:18:54 UTC	Document was created by Alliance for Better Health Contracting (philip.cassidy@abhealth.us) Device: Unknown on Unknown () IP number: 18.208.159.139 - IP Location: Ashburn, Virginia, United States

