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	KbPort LLC
Description of the purpose(s) for which Contractor will receive/access PII	Personal information collected and stored within SimEMR is limited to the Directory Information classification of data (First Name, Last Name, email address; of which only email address is required (for authentication purposes)). Patient data created using SimEMR is simulated data for the purposes of education and does not include real ePHI or other protected data.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR Data
Contract Term	Contract Start Date 07/01/2021 Contract End Date 06/30/2022
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: SimEMR is a cloud-based, multi-tenant SaaS application hosted on Microsoft's Azure platform using Azure's web application architectural model which has the following components: resource group, app service app, app service plan, deployment slots, Azure DNS, Azure SQL database, logical server, Azure storage. Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: SimEMR is a cloud-based, multi-tenant SaaS application that utilizes data discrimination techniques to support client-data isolation. KbPort strives to adhere to information security principles and we actively incorporate industry standard best practices into our SDLC.
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.	KbPort strives to adhere to NIST cybersecurity standards across all solutions, whether exclusively on-premise, hybrid, or cloud-based.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	SimEMR is a cloud-based service hosted in a multi-tenant environment via Microsoft Azure and utilizes network and data security provided by Azure Security Center.
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.	KbPort employees receive comprehensive training in cybersecurity, data privacy, online privacy. KbPort employees also receive training on all company policies, especially those related to the handling and confidentiality of customer data.
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.	KbPort does not use subcontractors. Under the terms of employment, all KbPort employees are bound to the policies set forth by KbPort's employee handbook and all issued company policies.
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.	A senior executive of KbPort will notify a senior member of EAs leadership team within 24 hours of confirmation of the event and would include the known relevant details. The EA and KbPort will work cooperatively in determining an action plan, including any required notification of affected persons.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	KbPort works in accordance with the terms of the EAs contract, to provide backup copies of the institution's data when required/requested.
7	Describe your secure destruction practices and how certification will be provided to the EA.	KbPort shall ensure that it disposes of any and all data or information received from EA in a commercially reasonable manner. Written cert available upon request
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	KbPort offers mechanisms to support client -driven security analysis and has a strong reputation for collaboration with clients to meet client-specific or specialized needs.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	KbPort strives to adhere to NIST cybersecurity standards across all solutions, whether exclusively on-premise, hybrid, or cloud-based.

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]	Verified by PDFFiller Christopher J Comer 09/08/2021
[Printed Name]	Christopher J Comer
[Title]	Professional Services
Date:	09/08/2021

KBPORT LLC THIRD PARTY VENDOR FERPA COMPLIANCE POLICY

KbPort, in its role as a vendor to educational agencies and institutions (EAs), receives disclosures from the EAs of personally identifiable information (PII) contained in student records. Only information that is needed for KbPort to perform services outsourced to it by the EA is disclosed to KbPort. These disclosures are authorized under the Family Educational Rights and Privacy Act (FERPA), a federal statute that regulates the privacy of student records by EAs that receive financial assistance from the U.S. Department of Education. KbPort, as a contractor to the EA, receives the disclosures on the same basis as school officials employed by the EA, consistent with FERPA regulations, 34 CFR §99.31(a)(1)(i)(B). Consistent with those regulations, KbPort has a legitimate educational interest in the information to which it is given access because the information is needed to perform the outsourced service, and KbPort is under the direct control of the EA in using and maintaining the disclosed education records, consistent with the terms of its contract.

KbPort is subject to the same conditions on use and re-disclosure of education records that govern all school officials, as provided in 34 CFR §99.33. In particular, KbPort must ensure that only individuals that it employs or that are employed by its contractor, with legitimate educational interests – consistent with the purposes for which KbPort obtained the information -- obtain access to PII from education records it maintains on behalf of the district or institution. Further, in accordance with 34 CFR §99.33(a) and (b), KbPort may not re-disclose PII without consent of a parent or an eligible student (meaning a student who is 18 years old or above or is enrolled in postsecondary education) unless the agency or institution has authorized the re-disclosure under a FERPA exception and the agency or institution records the subsequent disclosure. An example of such a disclosure is when KbPort is requested by a school district to assist the district in the transfer of the student records from our system to another system.

KbPort will not sell or otherwise use or re-disclose education records for targeted advertising or marketing purposes. KbPort may use anonymized, non-PII data internally to improve the products and services it delivers to EAs.

KbPort employs technological and operational measures to ensure data security and privacy, including advanced security systems technology and physical access controls, privacy training for employees, and criminal background checks of employees. All data is housed within the United States. Details about the company policies which support the KbPort security programs are available to EAs under a non-disclosure agreement.

All employees of KbPort are required to sign an Acknowledgement and Agreement of Policies that commits the employees to comply with KbPort's data privacy and security policies and receive required security and privacy training, including commitments and training regarding the prohibition on disclosure of student data.

KbPort does not own any of the student data or district-created data within its products. These data within the products are property of, and under the control of the local educational agency. The collection, input, use, retention, disposal, and disclosure of any information in our software applications are controlled solely by the EAs which license our products. KbPort cannot delete, change, or disclose any information from our software applications controlled by the EA. Students who wish to retain possession and control of their own pupil-generated content should contact the EA. If the EA is unable to fulfil the request of the student, KbPort can assist at the direction and expense of the EA.

In the event any third party (including the eligible student or parent/guardian of the eligible student) seeks to access education records, KbPort will immediately inform the EA of such request in writing. KbPort shall not provide access to such data or information or respond to such requests unless compelled to do so by court order or lawfully issued subpoena from any court of competent jurisdiction or directed to do so by the EA. Should KbPort receive a court order or lawfully issued subpoena seeking the release of such data or information, KbPort shall provide immediate notification, along with a copy thereof, to the EA prior to releasing the requested data or information, unless such notification is prohibited by law or judicial and/or administrative order or subpoena.

If the EA is unable to fulfil a request of an eligible student or parent/guardian to review the student's records, KbPort can assist at the direction and expense of the EA. In such an event where a parent, legal guardian, or eligible student seeks to make changes to the data within our products parents, legal guardians, or eligible students shall follow the procedures established by the EA in accordance with FERPA. Generally, these procedures establish the right to request an amendment of the student's education records that the parent or eligible student believes is inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Parents or eligible students who wish to ask the EA to amend their child's or their education record should write an EA official (often a Principal or Superintendent), clearly identify the part of the record they want changed, and specify why it should be changed. If the EA decides not to amend the record as requested by the parent or eligible student, the EA will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures would be provided to the parent or eligible student when notified of the right to a hearing.

In the event KbPort becomes aware of a data breach or inadvertent disclosure of PII, KbPort shall take immediate steps to limit and mitigate such security breach to the extent possible. A senior executive of KbPort will notify a senior member of the affected EAs leadership team, ideally the Superintendent or similar chief executive. This typically will occur within 24 hours of confirmation of the event and would include the known relevant details. The EA and KbPort will work cooperatively in determining an action plan, including any required notification of affected persons. In the event that KbPort is at fault for the breach or disclosure, KbPort carries a cyber-liability insurance policy that provides for a number of potential remedies, such as credit monitoring for affected parties, fraud coverage, crisis management communications coverage, business interruption coverage, and data restoration coverage, among others.

In the event of termination of a license to use our products, KbPort works with the EA, in accordance of the terms of the EAs contract, to destroy all student records contained in our systems and then will permanently delete all archival or backup copies of the agency’s or institution’s data. KbPort shall not knowingly retain copies of any data or information received from EA once EA has directed KbPort as to how such information shall be returned and/or destroyed. Furthermore, KbPort shall ensure that it disposes of any and all data or information received from EA in a commercially reasonable manner that maintains the confidentiality of the contents of such records (e.g. shredding paper records, erasing and reformatting hard drives, erasing and/or physically destroying any portable electronic devices). At the request of the EA, KbPort will provide a written certification of destruction.

To the extent parents, guardians or students have questions regarding the content of, or privacy associated with, any applications used by the educational institution, please contact that agency or institution.

KbPort may, from time to time, update this policy to be in compliance with evolving state and federal laws and regulations. We will not materially change our policies and practices to make them less protective of your privacy without the written consent of the EA and the EA may rely upon any and enforce any current or prior version of this policy unless otherwise agreed to in writing.

KBPORT LLC DATA PRIVACY AND HANDLING POLICY

Purpose

Our **KbPort Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Scope

This policy refers to all parties (employees, job candidates, customers, students and instructors of customers, suppliers etc.) who provide any amount of information to us.

Employees of KbPort must follow this policy. Contractors, consultants, partners and any other external entity acting on our behalf or in conjunction with us are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

KbPort collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time, if such time is specified
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

With respect to personally identifiable information obtained from educational institutions, KbPort will act in accordance with its Third-Party Vendor FERPA Compliance Policy, which is attached to and incorporated into this Policy.

<u>Actions</u>

To exercise data protection, we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Privacy Policy

Your privacy is important to us. It is KbPort LLC's policy to respect your privacy regarding any information collected from you across our website, http://kbport.com, and other sites or applications provisioned, operated, or supported by KbPort LLC.

We only ask for personal information when we truly need it to provide a service to you. We collect it by fair and lawful means, with your knowledge and consent. We also let you know why we’re collecting it and how it will be used.

We only retain collected information for as long as necessary to provide you with your requested service. What data we store, we’ll protect within commercially acceptable means to prevent loss and theft, as well as unauthorized access, disclosure, copying, use or modification.

We do not share any personally identifying information publicly or with third-parties, except when required to by law.

Our website may link to external sites that are not operated by us. Please be aware that we have no control over the content and practices of these sites, and cannot accept responsibility or liability for their respective privacy policies.

You are free to refuse our request for your personal information, with the understanding that we may be unable to provide you with some of your desired services.

Your continued use of our website or of applications or services provisioned to you by KbPort LLC, will be regarded as acceptance of our practices around privacy and personal information. If you have any questions about how we handle user data and personal information, feel free to contact us.

Customer Responsibility

You and your agents are solely responsible for operation, maintenance, and data or materials that appear on or within the applications provisioned to you by KbPort LLC.

This policy is effective as of 1 June 2020.