

Addendum A

05/23/2024

**DATA PRIVACY PLAN AND
PARENTS' BILL OF RIGHTS FOR
DATA SECURITY AND PRIVACY**

Pursuant to Section 2-d of the Education Law, agreements entered between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information (“PII”) to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District’s Parents’ Bill of Rights for Data Security and Privacy.

As such, EMS LINQ (LINQ, or The Company) agrees that the following terms shall be incorporated into the licensing agreement for services (“the Agreement”) and it shall adhere to the following:

1. The Contactor’s storage, use and transmission of student and teacher/principal PII shall be consistent with the District’s Data Security and Privacy Policy available here: <https://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BNBQY66B8921>
2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.
3. The exclusive purpose for which the student data or teacher or principal data will be used under the Agreement is the operation of LINQ Nutrition Software as set forth in Paragraph 1(a) only for the term of the Agreement as set forth in Paragraph 2.
4. The Agreement shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:
 - a. PII data will be protected using encryption while in motion and at rest by:

Data in transit is encrypted using TLS 1.3. Data at rest is encrypted using platform\disk encryption. The database level uses Microsoft Transparent Data Encryption.
 - b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored by Microsoft SQL Server. The security of this data will be ensured by multiple levels of protection, including; limited access, continuous logging and monitoring, Malware protection, File Integrity Protection, a Web Application Firewall, and Intrusion Detection.
 - c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows:

Physical Access to the data center is controlled by the hosting company, which in this case is the Google Cloud Platform

5. The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Agreement.

- a. By initialing here _____ Contractor represents that it will not utilize any subcontractors or outside entities to provide services under the Agreement and shall not disclose any PII other than as required pursuant to paragraph 6 below.
- b. [IF SUBCONTRACTORS ARE USED DESCRIBE HOW CONTRACTOR WILL “MANAGE RELATIONSHIPS”]

LINQ has implemented and maintains a vendor and business partner oversight program that is designed to ensure that third parties involved in delivering LINQ’s solutions comply with LINQ’s security requirements.

That program requires all contracts with vendors or business partners to clearly address (a) the requirement for the vendor or business partner to meet LINQ’s information security standards, (b) the ability to perform independent audits of the effectiveness of internal control processes, and (c) the requirement to obtain and provide a third-party attestation report.

Disclosure of any confidential information to a vendor or business partner is provided only as needed and only if the vendor or business partner has implemented appropriate information security and confidentiality controls.

6. Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII 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). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows:

Upon hire and annually thereafter, all LINQ employees must successfully complete training courses covering basic information security practices. The training courses are designed to assist employees with identifying and responding to social engineering attacks and avoiding inappropriate security practices.

Development and Cloud Operations staff receive further training specific to product development, deployment, and management of secure applications. Additional security training is also provided to employees who handle Customer Data.

7. Contractor shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the New

York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.

8. Upon expiration of the Agreement, the PII will be returned to the District and/or destroyed. Specifically, the customer will have access to the system for 90 days for a post termination period. During that period LINQ will make available to the customer their data. After the post termination period LINQ will securely remove all customer data from all systems.
9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected in accordance with the procedures set forth in the FERPA regulations at 99 C.F.R. Part 34, Subpart C, §§99.20-99.22.
10. The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII. [DESCRIBE – below are minimum requirements]
 - a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the District's data privacy officer by phone and by email.
 - b. Contractor shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.
 - c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the District for the full cost of such notification.
 - d. The Company has established and documented an incident response plan and corresponding procedures to respond to incidents that involve suspected compromise of, or unauthorized access to, Customer Data or other Company information, or Company information systems. The incident response plan is tested annually to assess its effectiveness.

The Company maintains several different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting the Cloud Services team per defined and configured events, thresholds, or metric triggers. Incidents may also be reported by email. Users are made aware of their responsibility to report incidents and that reports will be investigated without any negative consequences for the reporting party.

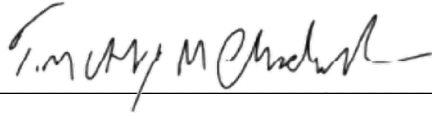
The Company has designated an incident response team to provide 24/7 event and incident monitoring and response services. The team use established incident classification, escalation, and notification processes for assessing an incident's criticality and severity, and corresponding escalation to appropriate groups, including privacy, legal, and executive management teams. Incident response

team members are trained on the Company's incident response plan and procedures.

Following any high severity incidents, LINQ performs post-mortem reviews to evaluate the lessons learned and identify potential areas of improvement.

11. A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov.

Contractor Signature: 
Name: Timothy M Chadwick, CISO

The District shall publish this contract addendum on its website.

Attachment A

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

Capital Region BOCES, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;
- A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov/data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov/data-privacy-security> by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website <https://www.capitalregionboces.org/>.