EXHIBIT B

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	Propio LS, LLC
Description of the purpose(s) for which Contractor will receive/access PII	**Propio Language Services receives and accesses Personally Identifiable Information (PII) solely for the purpose of delivering language interpretation and translation services to clients. PII, such as IP addresses, medical record numbers, dates, and URLs, may be processed as part of service delivery, quality assurance (e.g., reviewing call recordings), and to fulfill client-specific requirements such as intake questions for billing or service documentation. Access to PII is restricted to authorized personnel on a need-to-know basis, following the principle of least privilege. PII is only collected, stored, or transmitted as required to provide contracted services and is protected in accordance with applicable privacy laws and contractual obligations. Data is retained only as long as necessary for the intended service purpose and is securely disposed of after the retention period.**
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
Subcontractor Written Agreement Requirement	A 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 the Contractor. The contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Interpretation & Translation Services

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: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please see the following page.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	*Christopher Pesce*
[Printed Name]	Christopher Pesce
[Title]	CFO
Date:	10/13/2025

Propio mitigates data security and privacy risks through a comprehensive framework of technical, organizational, and administrative controls. All sensitive data, including PII and PHI, is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher. Access to data is strictly role-based, requires manager approval, and is logged and audited for traceability. Multi-factor authentication is enforced for internal applications, and the principle of least privilege is applied to all user accounts, including offshore resources. Data is logically segregated by Client ID and Access ID, ensuring client data is not combined or accessible by unauthorized parties. Regular security training, phishing simulations, and incident response drills are conducted for all personnel. Data Loss Prevention (DLP) solutions, endpoint protection, and secure file sharing are implemented across all endpoints. Propio maintains compliance with HIPAA, GDPR, CCPA, and holds certifications such as SOC 2 Type 2 and HiTrust. Continuous monitoring, regular audits, and prompt application of security patches further reduce risk. Privacy impact assessments and risk assessments are performed regularly, and privacy policies are reviewed and updated to reflect regulatory changes. In the event of a breach, an incident response plan ensures rapid containment, investigation, and notification as required by law. These measures collectively ensure that data security and privacy risks are proactively managed without compromising the security or integrity of the data.