

Raw student text never reaches any AI model.

That is not a policy commitment. That is the architecture.

1. PRODUCT AND COMPANY IDENTIFICATION

Product	XODA
Product Description	Diagnostic system for K–8 bilingual mathematics assessment
Canonical Positioning	The first diagnostic system built to separate a student’s mathematical ability from their language development stage.
Developer	mar&mar ideas products & more, LLC (dba QuizMyBrainz)
Headquarters	Fort Worth, Texas, USA
Stage	Research deployment (NSF SBIR Phase I submission in preparation)
Principal Investigator	Mario Oscar Pureco-Razo · oscarpureco@quizmybrainz.com
Co-Principal Investigator	Antonieta Ceron-Ponce · antonieta@quizmybrainz.com
Data Privacy Contact	oscarpureco@quizmybrainz.com

2. WHAT XODA DOES AND DOES NOT DO WITH STUDENT WRITING

GUARANTEES, NOT OPERATIONS

The XODA system incorporates a proprietary deterministic ruleset.

XODA DOES	XODA DOES NOT
<ul style="list-style-type: none"> ✓ Produce a language development stage classification. ✓ Produce a mathematical cognitive signal classification. ✓ Return those classifications to the teacher. ✓ Operate under FERPA governance and HIPAA Safe Harbor de-identification methodology. 	<ul style="list-style-type: none"> × Send student writing to any AI model, cloud API, or external service. × Retain raw student text. × Collect or store student names, IDs, or any re-identifiable attribute. × Share data with any third-party vendor or contractor. × Produce clinical diagnoses or SLD determinations.

3. DATA HANDLING SUMMARY

DATA TYPE	COLLECTED	PROCESSED	RETAINED
Raw student writing (verbatim text)	Yes — enters the system	De-identified internally	Never
Student name or ID	No	No	No
Personally identifiable information	No	No	No
Anonymized language signals	No raw text	Internal classification	Research corpus only
Mathematical cognitive signal	No raw text	Internal classification	Classification output only
District name in publications	No	No	Sealed under confidentiality
Audio, video, or biometric data	Never collected	—	—

All data handling complies with FERPA (20 U.S.C. § 1232g) and the HIPAA Safe Harbor de-identification standard (45 CFR §164.514(b)(2)). No student-identifiable data is used in any published research output.

4. COMPLIANCE FRAMEWORKS

- **FERPA** — Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g. All student educational records are governed by FERPA authorization held by the participating district. XODA never receives or processes data outside the scope of district-authorized research protocols.
- **HIPAA Safe Harbor** — 45 CFR §164.514(b)(2). De-identification methodology applied to all data under a separate data governance protocol adapted for educational data under FERPA.
- **COPPA** — Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506. Applicable to users under age 13. Architectural compliance: no personally identifiable information is collected, stored, or transmitted.
- **State-level compliance** — District-level student data privacy requirements (including but not limited to Texas Education Code frameworks) are satisfied at the district governance layer under district IRB authorization. XODA complies with district data agreements in force at each deployment site.

5. RESEARCH GOVERNANCE

All XODA deployments are conducted under district IRB authorization. The research protocol defines what data is collected, who has access, for how long, and under what governance.

District identity is sealed in all published research output. District identification is available only to IRB reviewers and journal editors under sealed confidentiality.

An IRB Authorization Scope Summary is available to district legal teams on request. Contact the Principal Investigator directly at oscarpureco@quizmybrainz.com.

6. ACCESS, RIGHTS, AND INCIDENT RESPONSE

WHO CAN ACCESS STUDENT DATA

The research team only — PI and Co-PI. No vendor, no cloud service, no external contractor receives student data under any circumstances. This is not a contractual restriction. It is a structural property of the XODA system.

DATA SUBJECT RIGHTS

Because no student-identifiable data is collected, retained, or transmitted, most data subject rights (access, correction, deletion) are architecturally satisfied: there is no retained record linked to a specific student to access, correct, or delete. Questions may be directed to the PI.

INCIDENT RESPONSE

In the event of a suspected data incident, QuizMyBrainz will notify the participating district’s designated data privacy coordinator within 72 hours of discovery. The architectural posture of the system (no raw student text retained, no student-identity data stored) limits the surface area of conventional breach scenarios, but incident notification commitments apply regardless.

7. VERIFICATION AND CONTACT

DIRECT CONTACTS	AVAILABLE ON REQUEST
<p>Principal Investigator Mario Oscar Pureco-Razo oscarpureco@quizmybrainz.com</p> <p>Co-Principal Investigator Antonieta Ceron-Ponce antonieta@quizmybrainz.com</p>	<ul style="list-style-type: none"> › Signed copy of this Data Privacy Sheet on QuizMyBrainz letterhead › IRB Authorization Scope Summary › District data agreement template › Architectural compliance walkthrough (for district technical review)

Raw student text never reaches any AI model.

This is an architectural guarantee, not a policy.

FERPA and HIPAA Safe Harbor compliant.