STRATA STRENGTH LLC

ATHLETE HEALTH & PERFORMANCE PLATFORM

DATA PRIVACY POLICY

FERPA & HIPAA Data Privacy Policy

How Strata collects, protects, restricts, and returns student-athlete data

Prepared for school administrators and legal counsel

Presented by **Michael Gordon, M.Ed, AT, CSCS** · Founder, Strata Strength LLC · Head Athletic Trainer, St. Xavier High School

CONFIDENTIAL · FOR LEGAL REVIEW

STRATA

by Strata Strength LLC · All-in-One Athlete Management Platform

Version 1.0 · November 2026 · stratastrength.net

mgordon@stratastrength.net

Entity: Strata Strength LLC ("Strata," "we," "us") **Applies to:** All client schools and organizations and their authorized users **Version:** 1.0 · August 2026 · stratastrength.net

> This Policy states how Strata collects, uses, protects, restricts, retains, and returns student-athlete information on behalf of the schools it serves. It is written to be consistent with Strata's *Security, Privacy & Compliance White Paper* and with the representations made on stratastrength.net. It is a statement of Strata's data practices and **does not constitute legal advice**; each school's counsel remains responsible for the school's own compliance determinations.

---

1. Our core commitments

1. **The school owns its data.** Strata processes student information solely on the school's behalf and at its direction.
2. **We never sell student data**, use it for advertising, or use it for any purpose other than providing the service.
3. **Least privilege.** Access is restricted by role; sensitive medical information is available only to authorized sports-medicine and physician roles.
4. **Security by design.** Data is encrypted in transit and at rest, isolated per school, and access is audited.
5. **Data minimization for AI.** Optional AI features send only what the task needs. Some send nothing identifiable; others, such as reading an uploaded doctor's note or drafting a message about a specific injury, necessarily include the student's name and health detail. The provider is contractually barred from training on it. A school may choose the no-PHI-to-AI setting or turn AI off entirely.
6. **Transparency and return.** Schools can export their data at any time, and we return/delete it on termination.

---

2. Definitions

- **FERPA**: the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99), which governs **education records** maintained by a school.
- **Education record / treatment record**: records maintained by the school (or a party acting for it) relating to a student, including athletic-training/health records the school maintains.
- **School Official**: a party to whom a school has outsourced an institutional service, under the school's **direct control**, with a **legitimate educational interest** in the records (34 CFR § 99.31(a)(1)).
- **HIPAA**: the Health Insurance Portability and Accountability Act and its Privacy/Security Rules.
- **PHI (Protected Health Information)**: individually identifiable health information held by a HIPAA covered entity or business associate. **FERPA education records and student treatment records are expressly excluded from the definition of PHI.**
- **De-identified data**: data from which name and direct identifiers have been removed.

---

3. Information we collect (on the school's behalf)

CATEGORY	EXAMPLES	WHO MAY ACCESS (BY ROLE)
Identity	Name, grade/graduation year, sport(s), jersey #, position, photo	School staff per role; the athlete
Performance	Test results, metrics, programming, wellness check-ins	AD/Admin, AT, physician, S&C, sport coach (own team), athlete
Health / medical	Injuries, return-to-play, allergies, medications, conditions, alert flags (e.g., EpiPen, asthma), concussion records	**Athletic Trainer (sports medicine) and team physician** (full); AD/Admin oversight; coaches see participation **status only**
Contacts	Parent/guardian and emergency-contact name, email, phone	School staff per role; surfaced for safety/communication
Account	Email, role, authentication credentials (passwords are stored only as secure hashes by our authentication provider)	The user; administrators (role/status only)

We collect only what is needed to provide the service. Health information is segregated and restricted as described in §6.

4. How we use information

- **Only to provide and operate the service** for the school (performance, health/injury, wellness, nutrition, recruiting outputs the school/athlete generate).
- **We do not** sell, rent, or share student data for advertising or any secondary commercial purpose; **we do not** use identifiable student data to train AI models.
- **Optional AI features** transmit only the data the task requires, and only when a user invokes the feature. For some features that is de-identified numbers; for others, such as reading an uploaded physical form or drafting a parent message about an injury, it includes the student's name and health detail. The school may disable AI features or select the no-PHI-to-AI setting.

5. FERPA policy

Strata operates as a **School Official** under FERPA:

- Strata performs an institutional service the school would otherwise perform itself, **under the school's direct control** as to the use and maintenance of records, and uses records **only** for the authorized purpose.
- Access within the platform is confined to users with a **legitimate educational interest**, as enforced by role-based access control.
- Strata **does not redisclose** education records to third parties except subprocessors necessary to deliver the service (§9), each bound by equivalent obligations, or as directed by the school or required by law.

- **Parental and eligible-student rights** (to inspect, review, and seek correction of records) are honored **through the school**, consistent with FERPA; Strata supports the school in fulfilling such requests and provides data export to enable them.

The designation is in writing. The school-official designation is not a marketing claim; it is a signed term. Section 5.7 of the Subscription Agreement has the school affirmatively designate Strata a school official with a legitimate educational interest, and Exhibit B (the Data Protection Addendum), Section B-1.1, carries the direct-control, permitted-use, and no-redisclosure conditions.

5A. State student-privacy law

Strata's agreement names the student-privacy and breach-notification statutes of the **school's own state**, not only Ohio. Whatever the state, Strata commits in Exhibit B (§B-1.4) that it will not sell, rent, or trade student data; will not use it for advertising, targeted advertising, or profiling; will not use it to train or improve a general artificial-intelligence model; and will not use it for any commercial purpose other than running the platform for the school.

STATE	STUDENT-PRIVACY LAW NAMED IN THE AGREEMENT	BREACH-NOTIFICATION LAW NAMED
Ohio	Ohio Rev. Code § 3319.321	Ohio Rev. Code § 1347.12 (public agencies); § 1349.19
Kentucky	KRS 365.734. Strata additionally provides the **written certification of compliance** that KRS 365.734(3) requires, as a signed term of the agreement	KRS 365.732; KRS 61.931–61.934 where the school is a public agency (which also adds §B-3.4 to the addendum)
Indiana	Ind. Code § 20-33-7; § 20-26-21	Ind. Code § 24-4.9 et seq.

Schools in other states receive the same commitments with their own state's statutes named. A school whose district has its own student data privacy addendum may substitute or add it.

---

6. HIPAA policy

- **Most school athletic-training records are FERPA records that HIPAA excludes from PHI.** For a typical school, the athletic trainer (a sports-medicine provider acting for the school) documents student injuries under **FERPA, not HIPAA**.
- Strata nonetheless applies **safeguards modeled on the HIPAA Security Rule**: access controls and unique user identification, encryption in transit and at rest, audit controls, and authentication/session security, to all health-related information, regardless of which statute governs.
- **If a school's counsel determines HIPAA applies** to a given data flow (e.g., a separately HIPAA-covered provider or covered transactions), Strata will act as a **Business Associate** and execute a **Business Associate Agreement (BAA)** with the school, and will ensure a corresponding BAA is in place with its hosting subprocessor before such data is onboarded.

---

7. Access control & medical-data segregation

- **Role-based least privilege.** Every account holds one role; each sensitive view/action checks a permission.

- **Students, parents and faculty are limited to their own records by the database itself**: the school-wide tables answer only to staff roles, and every student and parent read or save goes through a server-checked door that returns only what is theirs. A parent's access is to their own child, through a controlled, revocable mechanism.
- **Coaches and strength staff see only participation status** (cleared / limited / out) in the application, never clinical medical detail. Extending the database limits to coach accounts is in progress.
- **The clinical medical record** (notes, medications, mechanism, concussion specifics, RED-S) is shown only to the **athletic-training and physician** roles.
- **Per-school isolation** is enforced at the database level (Row-Level Security): no school can access another school's data.

8. Security safeguards

- **Encryption:** TLS in transit; AES-256 at rest.
- **Isolation:** database-enforced per-school Row-Level Security.
- **Authentication:** individual accounts; two-factor authentication available; secure password reset; passwords stored only as secure hashes by the authentication provider.
- **Auditing:** sensitive actions (access, changes, role changes, exports) are logged with user and timestamp.
- **Backups & recovery:** daily backups, a nightly encrypted archive, and a full restore tested November 5, 2026.
- **Secrets:** server-side only; never exposed in the browser.

9. Subprocessors

Strata uses the following subprocessors, each bound to security and breach-notification obligations:

SUBPROCESSOR	FUNCTION	DATA	POSTURE
Supabase (on AWS)	Database & authentication	All application data	SOC 2 Type II; encryption; HIPAA-eligible under BAA
Vercel (on AWS)	Hosting & server functions	Data in transit	SOC 2 Type II; TLS; DDoS mitigation
Amazon Web Services	Cloud infrastructure	Hosts the above	ISO 27001; SOC 1/2/3
Resend	Transactional email	Names, emails and the message being sent, including short safety alerts (for example a red-flag wellness check-in or a concussion check-in reminder)	TLS

SUBPROCESSOR	FUNCTION	DATA	POSTURE
Anthropic (Claude)	Optional AI features: reading uploaded documents, drafting notes, summaries	Only the information needed for the task; may include health information when the school enables these features in standard mode	No model training; zero or limited retention; server-proxied. **No business associate agreement is in place with this provider.** Schools that require one should select the no-PHI-to-AI setting or run Strata with no AI
OpenAI *(only if a school configures it)*	Same optional AI features	Same as above	Same as above
Groq / OpenAI Whisper	Optional voice-to-text for staff notes	Dictated audio	No model training; server-proxied; Groq zero data retention on; blocked by the no-PHI-to-AI setting

About AI features. Some optional features use artificial intelligence to help staff work faster, for example reading an uploaded physical form or drafting a note home. When your school turns these on, only the specific information needed for that task is sent securely to the AI provider named above, which is contractually prohibited from training on it and uses it only to return the result. Strata does not store the content of these requests. Your school can turn AI features off at any time, or choose the strict **no-PHI-to-AI** setting, under which no health information is sent to AI. The no-PHI-to-AI setting also turns off voice dictation, which uses an outside speech service.

A current subprocessor list and Data Processing Addendum are available to schools on request.

10. Data retention, return & deletion

- Strata retains school data for the duration of the service relationship to provide the service.
- Schools may **export** their data at any time in standard formats.
- On termination, Strata will **return and/or delete** the school's data within a defined period set in the agreement.

11. Breach notification

Strata maintains application-level audit logging and relies on its subprocessors' infrastructure monitoring. Upon a confirmed breach affecting a school's data, Strata will notify the school **as soon as reasonably practicable following discovery and within the period its state law requires**, consistent with FERPA expectations and the state breach statute named in its agreement (see §5A). The notice includes what Strata knows, so the school can meet its own notification duties. Subprocessors are contractually obligated to notify Strata of incidents affecting their platforms.

12. Student & parent rights

Because students are generally minors, rights are exercised **through the school**:

- **Inspect & review** records, and **request correction**, via the school; Strata supports fulfillment and provides export.
- **Parent access** is limited to the parent's own child and is provisioned/revoked by the school.

13. Children's privacy (COPPA)

Strata's services are provided to **schools** for students, predominantly of high-school age. Strata does not knowingly collect information directly from children under 13 outside the school context. Where any user under 13 is involved, the school provides the necessary authorization consistent with COPPA and FERPA.

14. Changes to this Policy

We may update this Policy to reflect changes in our practices or legal requirements. Material changes will be communicated to client schools. The version and date appear at the top of this document.

15. Contact

Questions about this Policy, data requests, or security matters may be directed to Strata's point of contact:

Michael Gordon, M.Ed, AT, CSCS Founder, Strata Strength LLC mgordon@stratastrength.net · stratastrength.net

Strata will finalize agreement terms (including FERPA school-official terms, any applicable BAA, indemnification, and insurance) with each school as described in the accompanying white paper.