

STRATA STRENGTH LLC

ATHLETE HEALTH & PERFORMANCE PLATFORM

SECURITY · PRIVACY · COMPLIANCE

Data Protection & Compliance White Paper

Liability, FERPA & HIPAA protections for student-athlete management

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

Subject: Data protection, liability posture, and FERPA / HIPAA alignment for student-athlete management **Version:** 1.0 · August 2026 · stratastrength.net

> **Purpose & scope.** This document explains how the Strata platform protects student-athlete information and supports the school's legal and regulatory obligations. It is a technical and operational overview written to assist your school's administration and legal counsel in their review **prior to onboarding live student data.** Items marked `CONFIRM W/ COUNSEL` or `ACTION ITEM` identify decisions or agreements the school and Strata should finalize together.

Terminology (please read first)

To avoid a common misreading, two roles in this document are distinct healthcare/coaching functions and are kept separate throughout the platform:

- **Athletic Trainer (AT / ATC): Sports Medicine.** A certified/licensed **healthcare provider** responsible for injury evaluation and care, rehabilitation, concussion management, and return-to-play. This is the clinical/medical role, and it is the role with access to the protected medical records described below. **"Athletic Training" in this document always means sports medicine, not weight-room training.**
- **Strength & Conditioning Coach (S&C).** The **performance/weight-room** role: testing, programming, and physical development. The S&C role is deliberately **excluded** from the clinical medical vault; it sees performance data and participation status only.

Wherever this paper refers to "athletic-training records," "clinical," or "medical" information, it means the **sports-medicine** record maintained by the AT/ATC and team physician.

---

1. Executive summary

Strata is an all-in-one athlete-management platform (strength & performance, health/injury, wellness, and nutrition). It was designed from the start around three principles that map directly to the school's legal interests:

1. **Least-privilege access.** Every user sees only what their role legitimately requires. Coaches never see clinical medical detail; only the athletic-training and medical staff do.
2. **Segregation of medical information.** Sensitive health data is walled off from the general performance data and is visible only to authorized clinical roles.
3. **Auditability.** Sensitive actions are logged, creating an accountability trail that supports both compliance and the school's standard-of-care documentation.

For a high school like your school, the athletic-training and student-health records Strata handles are, in the substantial majority of cases, **education records governed by FERPA, not HIPAA** (see §6). Strata is built to operate within the FERPA "school official" framework while simultaneously applying **technical safeguards modeled on the HIPAA Security Rule** (encryption, access controls, audit logging), so the school is well-positioned under either analysis.

1.1 Protections for the school: at a glance

Every protection in this document, mapped to the concern it answers:

THE SCHOOL'S CONCERN	HOW YOUR SCHOOL IS PROTECTED	SECTION
Who can see a student's **medical** information?	Restricted to the **Athletic Trainer (sports medicine) and team physician**. Coaches and strength staff see only participation status (cleared / limited / out).	§3, §4
Could **another school** see our data?	**No.** Per-school isolation is enforced **by the database itself** (Row-Level Security), not just the interface. A breach at one school cannot expose another.	§2.3, §3.2
Could a student's data be **hacked / stolen**?	No system is unhackable, but Strata layers multiple independent defenses and **contains** any single failure; the most sensitive medical data is the hardest to reach; data is encrypted in transit and at rest.	§2.3
Are we **FERPA**-compliant?	Strata operates under the FERPA **school-official** model: the school **owns and controls** the data; no secondary use; no sale.	§5
Does **HIPAA** apply, and are we covered?	For a high school, these are **FERPA records that HIPAA excludes**, so no BAA is needed; Strata applies safeguards modeled on the HIPAA Security Rule regardless and will sign a **BAA** if counsel finds HIPAA applies.	§6
Does **AI** expose student info?	**Only where the school allows it.** Some AI features send nothing identifiable. Others, like reading a doctor's note or drafting a parent message, send the name and health detail. A school can block those with the **no-PHI-to-AI** setting or turn AI off.	§11
What about **liability** if an injury is mismanaged?	Strata produces a **documented, time-stamped** record (injury logs, return-to-play staging, clearances, audit trail), the school's strongest position in any dispute.	§8
Will the vendor **sell or misuse** our data?	Contractually prohibited: **no sale, no advertising, no secondary use.** The school owns the data.	§5, §10
What happens in a **breach**?	Prompt notification commitment to the school, consistent with FERPA and Ohio breach law; automated database backups.	§2.4, §10
What if we **leave** Strata?	The school can **export** its data, and the agreement requires **return and/or deletion** on termination.	§10
If a **Strata failure** harms us, are we protected?	The agreement will include **indemnification** and Strata-maintained **cyber-liability / E&O insurance**.	§10.1

The remainder of this document details each item. Section §2.3 specifically addresses the "can someone hack in?" question, and §10.1 addresses the school's contractual and financial protections.

2. Data architecture & hosting

LAYER	PROVIDER	PROTECTION
Application database & authentication	**Supabase** (managed PostgreSQL)	Encryption **at rest** (AES-256) and **in transit** (TLS 1.2+); per-row access control (see §3)
Application hosting & server functions	**Vercel**	Served exclusively over **HTTPS/TLS**; server-side secrets never exposed to the browser
Underlying infrastructure	Cloud infrastructure (US-based regions)	Physical and network security inherited from enterprise cloud provider

Key properties:

- **Data in transit is encrypted** end-to-end over TLS. The application is not served over unencrypted HTTP.
- **Data at rest is encrypted** in the managed database.
- **Secrets (API keys, service credentials) live server-side only**: they are stored as protected environment variables and are never shipped to, or visible in, the athlete's or staff member's browser.
- **US data residency.** Data is hosted in United States cloud regions. `CONFIRM W/ COUNSEL` if any data-residency commitment must be contractually fixed.
- **No advertising trackers / no data sale.** Strata does not sell, rent, or share student data for advertising or any secondary commercial purpose.

For the HIPAA-covered scenarios in §6 (a college health center, or one of the two narrow high-school exceptions): **no BAA is in place today.** Before any HIPAA-covered data is onboarded, Strata signs a **Business Associate Agreement (BAA)** with the customer and moves that customer to hosting and AI covered by the providers' own BAAs (a separate environment, built and tested locally in November 2026). For a high school's own athletic training records, no BAA is required, because those are FERPA education records rather than PHI.

2.1 Hosting providers, certifications & subprocessors

Strata is built on established, independently-audited infrastructure providers rather than self-managed servers. The third parties that may process your school data ("subprocessors") are:

SUBPROCESSOR	FUNCTION	DATA IT TOUCHES	SECURITY POSTURE
Supabase (runs on AWS)	Application database & authentication	All application data	SOC 2 Type II; encryption at rest (AES-256) & in transit (TLS); Row-Level Security; HIPAA-eligible under BAA

SUBPROCESSOR	FUNCTION	DATA IT TOUCHES	SECURITY POSTURE
Vercel (runs on AWS)	Application hosting & server functions	Data in transit through the app	SOC 2 Type II; automatic HTTPS/TLS; DDoS mitigation; encrypted secret storage
Amazon Web Services	Underlying cloud infrastructure	Hosts the above	ISO 27001, SOC 1/2/3; enterprise physical & network security
Resend	Transactional email (invitations, sign-in codes, safety alerts)	Names, email addresses and the message being sent, including short safety alerts (for example a red-flag wellness check-in or a concussion check-in reminder)	TLS; reputable transactional-email provider
Anthropic / OpenAI	*Optional* AI features (if enabled)	Only what the task requires. De-identified numbers for some features; for document reading and parent-message drafting, the student name and health detail	Accessed via server-side proxy; no training on our data; no-PHI-to-AI setting available (see §11)
Groq	*Optional* voice dictation into staff notes	The dictated audio, only when a staff member taps Dictate	Server-proxied; zero data retention turned on; blocked by the no-PHI-to-AI setting

Certifications above reflect each provider's **published compliance documentation**. Supabase, Vercel and AWS each publish their own SOC 2 Type II report through their own trust portals. ACTION ITEM your school may obtain these reports and DPAs for its files, and Strata will provide its own DPA covering the subprocessors above.

2.2 Shared-responsibility model

Security on a modern platform is layered, and it is useful for counsel to see who is responsible for what:

LAYER	RESPONSIBLE PARTY	EXAMPLES
Physical & host infrastructure	**AWS**	Data-center security, hardware, network
Managed platform	**Supabase / Vercel**	Patching, platform hardening, TLS, DDoS, backups
Application	**Strata**	Access-control rules, organization isolation (RLS), encryption configuration, secrets management, audit logging, de-identification

LAYER	RESPONSIBLE PARTY	EXAMPLES
Account & usage	**your school**	Assigning correct roles (least privilege), enabling 2FA, protecting credentials, off-boarding departed staff

This is the same shared-responsibility model under which established school platforms (including student-registration and health-forms systems such as Final Forms) operate. Strata's controls are consistent with that established posture.

2.3 Can a student's data be "hacked"? An honest threat model

No internet-connected system (Strata, Final Forms, a school's own student-information system, or otherwise) can truthfully claim to be unhackable. **Any vendor that promises absolute invulnerability should not be trusted.** Credible security is about (a) layering defenses so an attacker must defeat many independent controls, and (b) ensuring that if any single control fails, the damage is **contained**. Strata is built on both principles.

The layers an attacker would have to defeat:

1. **Transport encryption (TLS).** All traffic is encrypted; intercepted traffic is unreadable.
2. **Every request is checked.** The database is reached through the hosting provider's encrypted endpoints. Every request needs a key and passes the database's own row-level security, so there is no anonymous access to any record.
3. **Authentication.** A valid email **and** password are required, with **two-factor authentication available** as a second factor.
4. **Organization isolation (Row-Level Security).** Even a *successfully authenticated* account is confined by the database itself to **its own school's data**. A your school account, or an attacker using one) **cannot read another school's records**, and a breach at one school does not expose any other.
5. **Role-based least privilege.** Students, parents and faculty are confined **by the database itself** to their own records: the school-wide tables answer only to staff roles, and a student's reads and saves go through a server-checked door that returns only what is theirs. Among staff, the application limits each role to what it needs: the clinical medical record is shown only to the athletic-training and physician roles, and coaches see participation status. Extending the database limits to coach accounts, so a coach's sign-in reaches only their own teams' non-clinical records, is in progress.
6. **Encryption at rest.** The stored data is encrypted on disk.

Containment ("blast radius"). Because of layers 4 and 5, a compromised student, parent or faculty credential reaches only that person's own records, and no credential at one school reaches another school. The broadest exposure is a compromised staff credential. Two-step sign-in is available on every staff account, and Athletic Trainers and physicians are prompted to set it up; school Google or Microsoft sign-in uses the school's own two-step.

The most realistic risk for *any* SaaS (including Final Forms) is a stolen user password (e.g., a staff member phished outside the system). Strata mitigates this with: two-factor authentication, least-privilege roles that limit what any one account can reach, an **audit trail** that records access for after-the-fact review, staged onboarding, and secure password-reset. The school's adoption of 2FA and good credential hygiene (its part of the shared-responsibility model) is the single highest-value protection here, and Strata supports it.

Bottom line for counsel: Strata cannot promise that no breach is ever possible (no honest vendor can), but it is engineered so that (1) breaking in requires defeating multiple independent controls, (2) a single failure is contained to a narrow scope, and (3) the most sensitive medical information is the hardest data to reach. This posture is consistent with, and in several respects stronger than (e.g., database-enforced per-school isolation and a no-PHI-to-AI setting enforced at the server), the platforms schools already entrust with the same student data.

2.4 Breach detection & notification

- **Monitoring & logging.** The platform providers maintain infrastructure monitoring; Strata maintains application-level audit logging (§8) of sensitive actions.
- **Backups & recovery.** The managed database is backed up automatically, which limits data-loss exposure (including from ransomware-style events). Point-in-time recovery is available on our hosting platform as an upgrade and is not yet active; ask for our current backup frequency and retention window.
- **Notification commitment.** Exhibit B of the Subscription Agreement (§B-3.2) commits Strata to notify the school of a confirmed breach affecting its data **as soon as reasonably practicable following discovery and within the period required by law**, consistent with FERPA expectations and the breach-notification statute of **the school's own state**, which the agreement names by citation (Ohio, Kentucky, and Indiana are covered today; other states are added the same way). Strata's subprocessors are likewise contractually obligated to notify Strata of incidents affecting their platforms.

---

3. Access control: least privilege by design

Strata enforces **role-based access control (RBAC)**. Each account is assigned exactly one role, and the application checks a permission for every sensitive view or action. In the app, coaches see availability, not medical records: the permission that gates clinical notes does not include the coach role.

3.1 Roles and what each can see

ROLE	PERFORMANCE DATA	INJURY STATUS (CLEARED / LIMITED / OUT)	CLINICAL DETAIL (NOTES, MEDS, MECHANISM, RED-S, CONCUSSION)	WELLNESS	USER MANAGEMENT
Athletic Director / Admin	✔	✔	Oversight-level injury info; deepest clinical notes limited to AD/AT/MD	✔	✔
Athletic Trainer	✔	✔	✔ (full, creates clinical records)	✔	✖
Team Physician / Medical Provider	✔	✔	✔ (full, clinical)	✔	✖
Strength & Conditioning Coach	✔	✔ (status only)	✖	✔	✖
Sport Coach	Their team only	✔ (status only)	✖	Summary only	✖

ROLE	PERFORMANCE DATA	INJURY STATUS (CLEARED / LIMITED / OUT)	CLINICAL DETAIL (NOTES, MEDS, MECHANISM, RED-S, CONCUSSION)	WELLNESS	USER MANAGEMENT
Parent / Guardian	Their own child only	Their own child only	✖	Their own child only	✖
Athlete	Their own data	Their own	Their own	Self-report	✖

The critical protections this enforces:

- **Coaches and strength staff never see clinical medical information.** They see only the actionable participation status (e.g., "limited," "cleared," "out"), exactly what a coach needs to keep a student safe, and nothing more.
- **The deepest clinical records** (SOAP notes, medications, RED-S, concussion specifics) are restricted to the athletic-training and medical roles.
- **Parents see only their own child**, through a controlled access mechanism (§7).

3.2 Organizational isolation (multi-tenancy)

Strata serves multiple schools from one platform, but every school's data is **isolated at the database level** using PostgreSQL **Row-Level Security (RLS)**. Each record is bound to an organization, and database policies make it impossible for a user authenticated to your school to query, read, or modify another organization's data, even via the API. Isolation is enforced by the database itself, not merely by the user interface.

---

4. Protection of medical & health information

- **Segregated medical vault.** Health information imported from registration systems (e.g., allergies, medications, existing conditions, EpiPen/inhaler/insulin and similar alert flags, emergency contacts) is stored against the athlete and surfaced **only to authorized clinical roles.**
- **Need-to-know surfacing.** Coaching staff see a participation status and, where appropriate, a minimal safety alert, not the underlying diagnosis or treatment record.
- **Documented return-to-play.** Injury logging and staged, documented return-to-play workflows (including concussion protocols) create a contemporaneous record that supports the school's standard of care.

---

5. FERPA alignment

The Family Educational Rights and Privacy Act (FERPA) governs **education records** maintained by a school. Strata is designed to operate within FERPA's framework:

- **School-official / service-provider model.** Strata functions as an outsourced service performing a function for which the school would otherwise use its own employees. Under FERPA (34 CFR § 99.31(a)(1)), a school may share education records with a party that (a) performs an institutional service, (b) is under the **direct control** of the school with respect to the use and maintenance of the records, and (c) uses the data only for the authorized purpose. All three conditions are written into the

Subscription Agreement: §5.7 has the school affirmatively **designate Strata a school official with a legitimate educational interest**, and Exhibit B §B-1.1 carries the direct-control and permitted-use conditions. CONFIRM W/ COUNSEL only whether the district requires its own student-data addendum in addition.

- **The school retains ownership and control.** your school remains the data owner. Strata processes the data solely to provide the service and at the school's direction.
- **No redisclosure; no secondary use.** Strata does not disclose student records to third parties for any purpose other than providing the contracted service, and does not use them for advertising or sale.
- **Access confined to legitimate educational interest.** The RBAC model (§3) operationally enforces the FERPA principle that access be limited to those with a legitimate educational interest.
- **Directory vs. non-directory information.** Recruiting outputs (e.g., athlete recruiting profiles) are generated under staff/athlete control; the school governs what is shared externally.

The written **agreement** memorializing the school-official designation, direct-control conditions, permitted use, data ownership, security obligations, breach notification, and return/deletion of data on termination is complete and is provided with this paper for counsel's review.

State student-privacy law. FERPA is the floor, not the ceiling. The agreement also names the student-privacy statute of the school's own state and binds Strata to it (Exhibit B §B-1.4): no sale, rent, or trade of student data; no advertising, targeted advertising, or profiling; no use of student data to train or improve a general artificial-intelligence model; no commercial purpose beyond running the platform for the school. For a **Kentucky** school, Strata additionally provides the written certification of compliance that KRS 365.734(3) requires, as a signed term rather than a separate letter, and for a Kentucky **public agency** the addendum adds the KRS 61.931–61.934 nonaffiliated-third-party terms (§B-3.4).

---

6. HIPAA considerations: the important nuance

A common misconception is that any "medical" data automatically triggers HIPAA. For a K-12 school, that is usually **not** the case:

- **FERPA generally controls, and HIPAA generally does not apply,** to health records the school maintains on its students. The HIPAA Privacy Rule **expressly excludes FERPA "education records" (and the "treatment records" of eligible students) from the definition of Protected Health Information (PHI).** (See the HHS/ED Joint Guidance on FERPA and HIPAA.) An athletic trainer employed by or acting for the school, documenting student injuries, is typically operating under **FERPA, not HIPAA.**
- **In practice, for a high school, this is settled.** A high school does not bill insurance electronically for health services and does not employ physicians who do, which is what makes an organization a HIPAA covered entity. Athletic training records at your school are FERPA education records. No BAA is required for Strata to be used as designed here.
- **The narrow exceptions, if either is true, tell us and we will execute a BAA:** the district bills Medicaid for school-based health services, or health services are delivered on campus by a separately covered provider (a hospital-run clinic, for example) whose records flow into Strata.
- **Colleges are different.** A university health center or sports-medicine department is ordinarily a HIPAA covered entity, and college athletic training records are commonly treatment records under HIPAA. No BAA is in place today. Before such a customer's records are onboarded, Strata signs a BAA with it as a Business Associate and hosts it in a separate environment covered by the providers' BAAs (built and tested locally, November 2026).

Strata's posture either way: Strata applies **safeguards modeled on the HIPAA Security Rule** regardless of which statute governs:

- Access controls and unique user identification (§3),
- Encryption in transit and at rest (§2),
- Audit controls (§8),
- Authentication and session security (§9).

If counsel determines HIPAA applies to any data flow, Strata will operate as a **Business Associate** and execute a **BAA** with the school, and will ensure a corresponding BAA is in place with its hosting subprocessor(s) before such data is onboarded.
ACTION ITEM

---

7. Parent / guardian access (minors)

Because most athletes are minors, parent access is deliberately constrained:

- Parents reach **only their own child's** information.
- Parent access is provisioned through a **controlled access mechanism** (school-issued access codes with the ability to revoke), not open self-registration into the roster.
- Parents see wellness/participation status and supportive information appropriate to a guardian , **not** the clinical record reserved for medical staff.

This supports both FERPA's treatment of parental rights for minor students and the school's interest in controlling who can see a given child's information.

---

8. Audit, accountability & standard-of-care support

- **Audit logging.** Sensitive events (e.g., logins, profile access, record changes, role changes, user additions/removals, data exports) are recorded with the acting user and timestamp, producing an **accountability trail.**
- **Documentation that supports the standard of care.** Injury logs, clearance/return-to-play staging, and concussion-protocol tracking create contemporaneous, time-stamped records. In a liability context, **documented, consistent process is the school's strongest position**: Strata is built to produce exactly that record, rather than relying on memory or scattered paper.
- **Role-change and access history** support after-the-fact review of who had access to what.

---

9. Authentication & account security

- **Individual accounts.** Every user authenticates with their own credentials; access is tied to a single role and (for staff/coaches) to specific sports/levels as appropriate.
- **Two-factor authentication (2FA)** is available for accounts, adding a second factor beyond the password.
- **Secure password reset** via a one-time, time-limited verification code delivered to the account's email (designed to remain reliable even through corporate email-link scanners).
- **Staged onboarding.** Schools can be configured and loaded **before** any invitations are sent, so a roster can be prepared privately and "opened" to users only when the school is ready , reducing premature exposure.
- **Server-side enforcement.** The walls between schools, the student and parent limits, the no-PHI-to-AI setting and AI usage limits are enforced on the server, not merely hidden in the interface. In the app, coaches see availability, not medical records.

---

10. Data ownership, retention & exit

- **The school owns its data.** Strata processes it on the school's behalf.
- **Export.** The school can export its data (e.g., rosters, reports) in standard formats.
- **Return/deletion on termination.** The agreement specifies return and/or deletion of your school's data upon termination and the timeframe for doing so (§5.5 and Exhibit B §B-5.2).
- **Breach notification.** The agreement specifies Strata's obligation to notify the school of a confirmed data breach, consistent with FERPA expectations and the breach-notification statute of the school's own state (Exhibit B §B-3.2).

10.1 Contractual & liability protections for the school

Technical safeguards protect the data; the **agreement** protects the school. Strata will enter a written agreement with your school that includes the following protections (counsel will finalize exact language and limits):

- **Data ownership & permitted use.** your school owns its data; Strata may use it **only** to provide the service, never for advertising, sale, model-training on identifiable data, or any secondary purpose.
- **Confidentiality & security obligations.** Strata is contractually bound to maintain the safeguards described in this paper.
- **Breach notification.** Written notice to the school upon a confirmed breach, as soon as reasonably practicable after discovery and within the period the school's own state law requires (§2.4).
- **State student-privacy commitments.** No sale, advertising, profiling, or AI model training on student data, bound to the school's state statute by name (Exhibit B §B-1.4).
- **Data return & deletion.** On termination, Strata will return and/or delete your school's data within a defined period.
- **Subprocessor flow-down.** Strata's subprocessors (§2.1) are bound to comparable security and breach-notification obligations.
- **Indemnification.** ACTION ITEM Strata will **indemnify** your school against losses arising from Strata's breach of its security/confidentiality obligations or its negligence. Scope and any caps to be finalized with counsel.
- **Cyber-liability / technology E&O insurance.** Strata is operated by **Strata Strength LLC**, a limited-liability entity, and **will maintain cyber-liability and technology errors-&-omissions insurance** (currently being bound), with a certificate of insurance available to your school on request. Coverage limits to be confirmed with counsel.

How Strata also *reduces* the school's own liability exposure. Beyond protecting data, Strata strengthens the school's position in the most common liability scenario, a dispute over how a student-athlete's injury or clearance was handled. By producing a **contemporaneous, time-stamped, access-controlled record** (injury logs, staged return-to-play, clearances, and an audit trail of who accessed what and when), Strata replaces memory and scattered paper with documented, consistent process, which is the school's strongest defense (§8).

10.2 Data availability & continuity: you will not lose access to your data

A frequent and fair concern is the mirror image of a breach: "*How do we know our data won't be lost, or locked inside a system we can't get to?*" Strata addresses this directly:

- **Export anytime, no lock-in.** The school can export its data (rosters, testing, reports) in **standard formats (e.g., CSV)** whenever it wants. Your data is never trapped in a proprietary black box.
- **Automated backups.** The managed database is backed up automatically, which protects against accidental deletion, corruption, and ransomware-style loss. Point-in-time recovery (restoring to an exact prior moment) is available on our hosting platform as an upgrade; ask for our current status and retention window.

- **Durable, isolated storage.** Each school's data persists independently in an enterprise-grade database (encrypted, replicated by the cloud provider). One school's actions cannot delete or corrupt another's.
- **Continuity if the relationship ends, or if Strata does.** The agreement commits Strata to **return a full export of the school's data** on request and on termination. Because the data is exportable in standard formats at any time, the school is never dependent on Strata's continued operation to retain access to its own records. ACTION ITEM Counsel may also request a data-return/escrow clause for added assurance.
- **No silent hostage of data.** Strata does not withhold a school's data; the school owns it and can retrieve it.

In short: the school's data is **backed up** (protected from loss), **exportable** (never locked in), and **contractually returnable** (protected from vendor dependence).

---

11. Optional AI features: how data is handled

Strata includes optional AI-assisted features (e.g., performance insights, programming suggestions). Some send nothing identifiable. Others, like reading a doctor's note or drafting a parent message, send the name and health detail. A school can block those with the **no-PHI-to-AI** setting or turn AI off.

- **Optional & staff-invoked.** AI features run only when a user explicitly invokes them; the school can disable them entirely.
- **Server-side proxy.** AI requests route through a server-side proxy, so the AI provider key is never exposed in the browser and usage can be governed and rate-limited centrally.
- **De-identified where the task allows.** Some features genuinely send nothing identifiable. The training-insight feature, for example, sends an *anonymized* profile (sport, level, position, gender, and performance scores) under a non-negotiable instruction that the model must not reference or store personal identifying information: a student appears as *"a 5'8", 215 lb freshman"*, never by name.
- **Other features necessarily send identifiable data, and we state that plainly.** Reading an uploaded doctor's note, physical form, or printed roster sends the document as it is, name included. Drafting a parent message sends the athlete's first name with the injury detail. Load monitoring names the athletes it flags. There is no way to perform those tasks without the identifiers, so the honest position is disclosure and contractual protection, not a claim of anonymity.
- **Data minimization.** Only the attributes needed for the requested task are included, and Strata stores none of the request content.
- **The school's control.** A per-school **no-PHI-to-AI** setting blocks the health-data features server-side, and AI can be turned off entirely. Schools requiring a business associate agreement for AI should use one of those two settings: **no BAA is currently in place with the AI provider.**
- CONFIRM W/ COUNSEL the school's preferred AI policy (allow de-identified performance insights / restrict further / disable). Strata will honor the school's choice.

---

12. Summary checklist for your school & counsel

#	ITEM	OWNER	STATUS
1	Execute the Subscription Agreement. FERPA "school official" terms (direct control, permitted use, ownership, security, breach notice, data return) are in the Agreement and Exhibit B (DPA)	School + Strata	Sign

#	ITEM	OWNER	STATUS
2	HIPAA: does not apply to a high school's own athletic training records (§6). Tell us if the district bills Medicaid for school-based services or an outside covered provider feeds records in	School	Note
3	BAA: available on request if either exception in §6 applies. No BAA is in place today; before such data is onboarded, Strata moves it to hosting and AI covered by the providers' BAAs	School + Strata	On request
4	Breach notification is in Exhibit B (B-3). Confirm data-residency expectations if the school has a written standard	School + Strata	Review
4a	State student-privacy terms are in Exhibit B (B-1.4), citing the school's own state statute. Tell us if the district requires its own student data privacy addendum instead	School's counsel	Review
5	Decide AI feature policy: full, no-PHI-to-AI, bring-your-own-key, or off (§2.5)	School	CONFIRM W/ COUNSEL
6	Confirm parent-access provisioning process aligns with school policy	School	Review
7	Confirm role assignments match staff duties (least privilege) before go-live	School	Review
8	**Indemnification** is in the Agreement (§9). Counsel to review	School's counsel	Review
9	Strata maintains **cyber-liability / tech E&O insurance** (§12.4) and furnishes a certificate on request	Strata	PENDING

13. About this document

This white paper describes Strata's architecture, controls, and design intent as of the version date above. Strata will work in good faith with your school to finalize the agreements and confirmations identified as ACTION ITEM / CONFIRM W/ COUNSEL above before live student data is onboarded.

Strata · Strata Strength LLC · stratastrength.net