

Security and Data Practices Summary

For IT, security, and legal reviewers. A plain statement of what the platform collects, what it never collects, and how employee privacy is protected. One page on purpose.

What the platform is

Human Aligned Health runs a four-week Thriving Challenge for employers: employees take a brief self-reflection reading (eight 0–10 self-ratings) at the start and close of the Challenge, engage with guided wellbeing content in between, and the employer receives a group-level picture of how their population is doing. It is a wellbeing measurement and engagement tool, not a medical service.

Data collected, and data never collected

Collected	Never collected
Work email address, used for sign-in and participation status only	Diagnoses, medical records, treatment or claims data
Self-report readings: eight whole-number self-ratings, 0–10, per reading	Biometric, genetic, or family health information
Usage events (content plays, completions), keyed to an anonymized identifier	Health history, prescriptions, or provider records

Privacy architecture

Individual readings are never shown to the employer. Group results render only when at least twelve people have completed a reading, a floor that exceeds the CMS public-reporting minimum, so no individual can be inferred from a group view. The one identity-level fact an employer can see is participation status, whether a person joined and completed their readings, and this is disclosed to each employee plainly before they begin. Readings and activity stay anonymized and aggregated; participation status is the only exception, and it never includes what anyone answered.

Regulatory posture

The Challenge is sold to and paid for by the employer directly, outside the employer's group health plan. It offers general wellbeing self-reflection and lifestyle content, not medical care, diagnosis, or treatment, and the platform does not create, receive, or maintain protected health information on behalf of a health plan or provider. Under HHS guidance on workplace wellness programs, HIPAA's rules attach to programs offered as part of a group health plan; programs offered by an employer directly, outside the plan, sit outside that scope. Our terms require that employers not tie Challenge participation to group health plan benefits (premiums, cost-sharing, or HSA/HRA contributions), which keeps that boundary intact. Participation is voluntary, and no genetic or family health information is requested at any point.

Security measures

Authentication is passwordless (single-use magic links to a verified work email), so no passwords are stored or breachable. Data is encrypted in transit (TLS) and at rest, hosted on Supabase managed infrastructure. Usage analytics are keyed to an anonymized identifier, separated from identity. Access to production data is role-restricted. Sign-in for each employer's Challenge is restricted to that employer's verified email domains.

Data lifecycle

Individuals can request deletion of their readings at any time. When a Challenge ends, the employer retains group-level results only; individual-level data remains private to each person. Full data handling practices: humanalignedhealth.com/security.

This summary describes the platform's structure and practices in plain language. It is provided for reviewer convenience and is not legal advice.