AimwellBio

Security & Compliance Statement

SOC 2 Type II Readiness · ISO/IEC 27001 ISMS · FHIN Data Governance

Version 1.0 · Effective April 20, 2026

Prepared by: John Morgan, CEO & Information Security Officer

✓ SOC 2 Controls Active **✓ ISO 27001 ISMS v1.0** **✓ FHIN Audit Log Live**

1. Executive Summary

AimwellBio is building the Federated Health Intelligence Network (FHIN) — a compliance-native physician data exchange platform designed to meet the security and governance standards required for institutional healthcare and sovereign-aligned data partnerships.

From inception, AimwellBio has engineered its systems against SOC 2 Trust Service Criteria and ISO/IEC 27001 Annex A controls — not as a retrofit, but as a foundational design principle. This document provides a transparent accounting of our current control posture, active implementations, and the structured path to formal third-party certification.

Attribute	Details
Organization	AimwellBio Inc.
Platform	FHIN — Federated Health Intelligence Network
Compliance Framework	SOC 2 Type II (AICPA) · ISO/IEC 27001:2022
ISMS Version	v1.0 — Effective April 20, 2026
Information Security Officer	John Morgan, CEO
Data Infrastructure	Supabase (SOC 2 certified) · Vercel (SOC 2 certified)
Audit Trail	fhin_audit_log — Supabase append-only event log
Observation Window	Started April 20, 2026 (SOC 2 Type II eligible ~Q4 2026)

2. SOC 2 Trust Service Criteria Mapping

The following table maps AimwellBio's FHIN system components to the AICPA SOC 2 Trust Service Criteria. Status reflects implemented controls as of April 20, 2026.

TSC	FHIN Component	Control Implemented	Status	Score
CC1.2	Policies & Procedures	Information Security Policy v1.0 documented at /admin/compliance-policies	✓ Done	95
CC6.1	Access Provisioning	FHIN_ADMIN_KEY auth on all privileged endpoints; 90-day rotation policy defined	✓ Done	88
CC6.2	Admin Authentication	Session-based auth on grand-admin; rolling access log in localStorage; MFA roadmap Q2 2026	⚠ Partial	70
CC6.3	Role-Based Access	Access Control Policy documented; admin roles defined; separation in roadmap	⚠ Partial	72
CC7.2	Audit Logging	fhin_audit_log table live in Supabase; fhin-apply and fhin-approve log all events	✓ Done	90
CC7.5	Incident Response	Incident Response Procedure documented (P1/P2/P3 severity, 72hr notification)	✓ Done	88
CC9.2	Vendor Risk	Vendor Register at /admin/vendor-register; 5 vendors documented with DPA status	✓ Done	82
P3.1	Privacy — Collection	Consent checkbox + privacy notice on all FHIN apply and onboarding forms	✓ Done	90
PI1.1	Processing Integrity	Server-side validation on fhin-apply; audit log records every state change	✓ Done	85
C1.1	Confidentiality at Rest	Supabase encrypts all data at rest (AES-256); RLS enabled on all FHIN tables	✓ Done	95
C1.2	Confidentiality in Transit	TLS 1.3 enforced on all endpoints via Supabase and Vercel infrastructure	✓ Done	95
A1.1	Availability	Vercel global CDN (99.99% SLA); Supabase managed Postgres with automatic failover	✓ Done	90

3. ISO/IEC 27001:2022 Annex A Controls

AimwellBio has implemented an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022. The following maps active controls to the FHIN system architecture.

Control	Domain	Implementation	Status	Evidence
A.5.1	IS Policy	Information Security Policy v1.0 — scope, classification, roles, review cycle	✓ Done	Policy doc
A.5.9	Asset Register	All systems, tables, API keys, and vendors enumerated in Vendor Register	✓ Done	Admin page
A.5.12	Info Classification	Four tiers: Public / Internal / Confidential / Restricted — defined in IS Policy	✓ Done	Policy doc
A.5.15	Access Control	Access Control Policy v1.0 — least privilege, credential rotation, access reviews	✓ Done	Policy doc
A.5.19	Supplier Security	Vendor Register with DPA status for Supabase, Anthropic, Vercel, Make.com, Airtable	✓ Done	Vendor reg
A.5.26	Incident Response	IRP v1.0 — P1 <1hr, P2 <4hr, P3 <24hr, GDPR 72hr breach notification	✓ Done	Policy doc
A.5.34	Privacy Protection	Consent checkbox on all data collection forms; Privacy Policy linked at point of collection	✓ Done	Live forms
A.8.2	Privileged Access	FHIN_ADMIN_KEY scoped to admin operations; rotation policy defined	⚠ Partial	Policy doc
A.8.5	Secure Auth	Session auth on admin portal; MFA implementation target Q2 2026	⚠ Partial	Roadmap
A.8.15	Logging	fhin_audit_log: append-only, 12 fields, all FHIN events logged with actor/resource/status	✓ Done	DB table
A.8.16	Monitoring	Supabase function logs; Vercel deployment monitoring; Execution Telemetry (migration pending)	⚠ Partial	Supabase
A.8.24	Cryptography	AES-256 at rest (Supabase); TLS 1.3 in transit; bcrypt for secrets via Supabase Vault	✓ Done	Infra

4. FHIN Data Governance

4.1 Data Classification

Tier	Data Type	Examples	Controls Applied
Public	Contributor profiles	Name, institution, publications, AI Score	Open read, no auth required
Internal	Operational data	Application status, member slugs, tier assignments	Admin auth required; audit logged
Confidential	PII + credentials	Email, phone, ORCID, LinkedIn, API keys	Encrypted at rest; RLS enforced; access logged
Restricted	PHI-adjacent	Clinical trial data, contribution payloads	Service role only; consent required; max audit trail

4.2 Audit Trail Architecture

Every FHIN system event is written to the fhin_audit_log table in Supabase. This provides an immutable, append-only audit trail suitable for SOC 2 evidence collection.

Field	Type	Purpose
event_type	text	Action identifier (e.g. fhin_application_submitted, fhin_application_approved)
actor_type	text	applicant | admin | system — identifies who triggered the event
actor_id	text	Email or admin identifier for human actors
resource_type	text	What was acted upon (fhin_application, fhin_member, etc.)
resource_id	text	UUID of the specific record affected
status	text	success | failure | blocked — outcome of the action
compliance_note	text	Human-readable SOC 2 / ISO control reference (e.g. “SOC2 P3.1 — consent given”)
metadata	jsonb	Structured context: name, org, role, error details, member_slug, etc.

5. Third-Party Vendor Risk Register

All vendors with access to AimwellBio data are documented below per ISO 27001 A.5.19 (Supplier Relationships). DPA status is current as of April 20, 2026.

Vendor	Role	Data Processed	Certification	DPA Action
Supabase	Database + Edge Functions	PII, applications, credentials	SOC 2 Type II ✓	⚠ Request at supabase.com/dpa
Anthropic	LLM — Claude API	Research queries, validation	SOC 2 (in progress)	⚠ Sign DPA at anthropic.com
Vercel	Frontend hosting + CDN	Web traffic, edge logs	SOC 2 Type II ✓	⚠ Request at vercel.com/legal
Make.com	Workflow automation	Lead data, FHIN webhooks	ISO 27001 ✓	✓ Review ToS completed
Airtable	CRM / Lead management	Name, email, inquiry data	SOC 2 Type II ✓	⚠ Available on Enterprise plan

Next vendor review date: July 20, 2026

6. Certification Roadmap

Phase	Timeline	Milestones	Outcome
Phase 1 — Foundation	Days 0–30 (Now)	Consent gates ✓ | Audit log ✓ | IS Policy ✓ | Access Policy ✓ | IRP ✓ | Vendor Register ✓	Controls Active
Phase 2 — ISMS	Days 31–90	Risk register | MFA implementation | Admin role separation | DPAs signed | Internal audit	ISO Eligible
Phase 3 — SOC 2 Window	Days 91–270	6-month behavioral observation | Continuous control monitoring | External auditor engaged	SOC 2 Audit Ready
Phase 4 — Certification	Q4 2026	SOC 2 Type II report issued | ISO 27001 certification audit | Public trust page	✓ Certified

AimwellBio does not treat compliance as a checkbox. We treat it as a market-entry weapon. Every data flow in FHIN was mapped against SOC 2 and ISO 27001 before a single line of production code was deployed. This document is the evidence.

7. Security Contact & Disclosure

Security inquiries, vulnerability disclosures, and compliance requests:

Email: corporate@aimwellbio.com

Website: aimwellbio.com/security

Response SLA: P1 security issues acknowledged within 24 hours

This document is reviewed quarterly. Last review: April 20, 2026. Next scheduled review: July 20, 2026.