VitaAI Systems — SOC 2 Risk Register

CC9 — Risk Mitigation · Version 1.0 · Effective June 5, 2026 · CONFIDENTIAL

Owner: Steven Wallace, CEO — Altnetix | Next Review: June 1, 2027 | Scope: VitaAI web app, API, Electron desktop, Azure infrastructure (Altnetix subscription)

1. Purpose and Scope

This Risk Register documents VitaAI's formal assessment of risks to the security, availability, processing integrity, confidentiality, and privacy of systems and data per the AICPA SOC 2 Trust Services Criteria CC9 (Risk Mitigation). It is reviewed annually and after any material security incident.

2. Risk Scoring Methodology

Risk Score = Likelihood (1–5) × Impact (1–5). Maximum score = 25.

Score	Risk Level	Action Required
1 – 5	**Low**	Accept. Monitor annually. No immediate action required.
6 – 12	**Medium**	Mitigate within 90 days. Assign owner. Quarterly progress review.
13 – 25	**High**	Immediate remediation plan within 30 days. CEO escalation required.

3. Risk Register

L = Likelihood (1–5) · I = Impact (1–5) · Score = L × I

ID	Risk Description	SOC 2	L	I	Score	Current Controls	Residual	Owner	Review	Status
R-001	Unauthorized access to PHI via compromised credentials	CC6.1, CC6.2	2	5	10	MSAL MFA, SAML SSO, account lockout (5 attempts / 15 min), 15-min JWT TTL, 12-char password policy (NIST 800-63B)	Low	CTO	2027-06-01	Mitigated
R-002	Insider threat — employee misuse of PHI access	CC6.3, CC6.6	2	5	10	RBAC (ProviderOnly / PatientOnly), immutable WORM audit log, hash-chained entries, App Insights anomaly alerts	Low	CTO	2027-06-01	Mitigated
R-003	Third-party breach via Azure infrastructure	CC9.2	1	5	5	Azure SOC 2 Type II certified, Azure BAA accepted, Managed Identity (no stored credentials), VitaDev01Vault Key Vault	Low	CEO	2027-06-01	Mitigated
R-004	Data loss / ransomware	A1.2, CC7.5	2	5	10	Azure SQL geo-redundant backups, Azure Blob soft-delete, BackupHealthService 4-hr verification, DR plan documented	Low	CTO	2027-06-01	Mitigated
R-005	SQL injection / API attack	CC6.8	2	5	10	InputSanitizationFilter (global), parameterized EF Core queries, rate limiting (10/min auth), CSP + X-Frame-Options: DENY	Low	CTO	2027-06-01	Mitigated
R-006	PHI transmitted unencrypted	CC6.7	1	5	5	TLS 1.3 / min TLS 1.2, HSTS 1-year preload, HTTPS redirect enforced, Cache-Control: no-store on all /api responses	Low	CTO	2027-06-01	Mitigated
R-007	PHI stored unencrypted at rest	C1.1, CC6.1	1	5	5	AES-256-GCM field encryption on all PHI columns, per-tenant DEK rotated annually, Azure Key Vault managed keys	Low	CTO	2027-06-01	Mitigated
R-008	Audit log tampering or deletion	CC7.2, CC7.3	2	4	8	WORM immutable blob (6-yr retention), hash-chained SQL entries, Service Bus outbox (no dropped events), separate vitaaiauditstorage account	Low	CTO	2027-06-01	Mitigated
R-009	Software change introduces security vulnerability	CC8.1	3	4	12	Azure DevOps CI/CD (PR required), TypeScript strict mode, .NET build validation, 3-stage deploy with approval gate, electron-updater integrity, Change Management Policy v1.0	Medium	CTO	2026-09-01	In Progress
R-010	Desktop app data leakage on shared workstation	CC6.6	2	4	8	15-min auto-logoff (Electron + web), session cleared on app quit, Cache-Control: no-store on all /api, cookies cleared on exit	Low	CTO	2027-06-01	Mitigated
R-011	Availability outage — API or Static Web App	A1.1, A1.2	2	3	6	Azure App Service (vita-dev-01) + Static Web App (vitaai-blank-ui), /health + /health/ready endpoints, App Insights anomaly alerts, BackupHealthService	Low	CTO	2027-06-01	Mitigated
R-012	AI clinical note accepted without provider review	PI1.4	2	5	10	Provider attestation required before signing, AI output labeled with warning banner, manual-only scribe (no auto-start), addendum system for post-sign corrections	Low	CMO	2027-06-01	Mitigated

4. Risk Acceptance Criteria

Low (1–5)	Accept. Monitor annually. No immediate action required.
Medium (6–12)	Mitigate within 90 days. Assign owner. Quarterly progress review.
High (13–25)	Immediate remediation plan within 30 days. CEO escalation required.
Critical (20+)	Stop-ship. No production deployment permitted until resolved.

5. Review Schedule

- Annual review: every June 1.
- Post-incident review: within 30 days of any confirmed security incident.
- On material system change: when new services, integrations, or data flows are added.
- On regulatory change: within 60 days of any applicable law or standard update.

6. Approvals

This Risk Register has been reviewed and approved by:

Role	Name	Signature	Date
Chief Executive Officer	Steven Wallace		June 5, 2026
Chief Technology Officer	TBD		_____