Remote–I

Risk Register (Abbreviated)

Document Type: Register

Version: 1.0 **Effective Date:** 12 December 2025

Owner: Remote-I Ltd – Technical Lead

Classification: Internal / Customer Assurance

Review Cycle: Quarterly and after incidents

Organisation: Remote-I Ltd
Company Number: 15293974
Registered Office: 45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB
Compliance Contact: compliance@remote-i.com
Data Protection Lead: Remote-I Ltd – Data Protection Lead

1. Purpose

This Risk Register summarises key security, privacy, operational and supplier risks relevant to Remote‑I. It supports NHS DSP Toolkit and ISO/IEC 27001 risk management evidence.

2. Scoring Method

Likelihood (L) and Impact (I) are scored 1 (Low) to 5 (High). Inherent risk rating = L×I. Residual risk reflects expected risk after controls.

3. Review

Risks are reviewed at least quarterly and after major incidents or material platform changes.

Risk ID	Category	Risk Description	Inherent (L×I)	Key Controls / Mitigations	Residual	Owner	Status	Next Review
R-01	Security	Credential compromise (admin) → unauthorised access	20	MFA; strong passwords; least privilege; monitoring; rapid offboarding	8	Tech Lead	Mitigated	2026-03-12
R-02	Security	Privilege escalation due to misconfigured roles	12	RBAC; access reviews; change control; audit logs	6	Tech Lead	Mitigated	2026-03-12
R-03	Privacy	Incidental patient identifiers entered into free-text	15	Minimisation guidance; SOPs/training; auditing; retention controls	9	DPL	In progress	2026-03-12
R-04	Availability	Hosting outage causing service unavailability	15	BCP/DRP; backups; supplier escalation	9	Tech Lead	Mitigated	2026-03-12
R-05	Integrity	Database corruption causing loss of governance evidence	10	Daily backups; restore tests; monitoring	5	Tech Lead	Mitigated	2026-03-12
R-06	Security	Web vulnerability exploited (OWASP class)	15	Patch mgmt; secure coding; monitoring; change control	9	Tech Lead	In progress	2026-03-12
R-07	Operational	Backup job failure undetected for multiple days	12	Backup verification; periodic review; alerting improvements	6	Tech Lead	In progress	2026-03-12
R-08	Supplier	Email/SMS provider outage delays notifications	9	Fallback channels; provider governance; graceful degradation	6	Tech Lead	Accepted	2026-03-12
R-09	Compliance	Insufficient evidence for procurement/audits	8	Audit logs; policy suite; governance exports; SoA; DPIA	4	Compliance	Mitigated	2026-03-12
R-10	Security	Insider misuse of authorised access	10	Least privilege; logging; access reviews; contractual controls	6	Customer/Admin	Shared	2026-03-12
R-11	Privacy	DSAR not handled within statutory timelines	8	Defined DSAR workflow; DPA; ticketing	4	DPL	Mitigated	2026-03-12

Risk ID	Category	Risk Description	Inherent (L×I)	Key Controls / Mitigations	Residual	Owner	Status	Next Review
R-12	Security	Secrets exposure through misconfiguration	10	Secrets isolation; permissions; rotation; change control	4	Tech Lead	Mitigated	2026-03-12
R-13	Supplier/Physical	Physical compromise at hosting provider	5	Supplier due diligence; contractual controls; provider physical security	3	Tech Lead	Accepted	2026-03-12
R-14	Operational	Key-person dependency impacts resilience	12	Runbooks; documented procedures; cross-training	8	Leadership	In progress	2026-03-12
R-15	Continuity	Destructive attack requires rebuild	10	Backups; DRP; incident response; credential rotation	6	Tech Lead	Mitigated	2026-03-12