RadPal

Security & Compliance Whitepaper

Prepared for institutional IT and security review · July 2026 · RadPal LLC

1. ABOUT RADPAL

RadPal is a **physician-supervised documentation productivity tool** for radiology reporting. It converts a radiologist's dictated findings into a draft report or impression; the radiologist reviews, edits, and signs every report. RadPal makes no autonomous clinical decisions, renders no diagnoses, and never inserts text without physician action. It runs as a standalone Windows desktop application alongside existing dictation software (e.g., PowerScribe, Fluency) and requires no PACS, RIS, or EHR integration, no DICOM image access, and no ingestion of patient demographics. RadPal is not a medical device and is not FDA-cleared.

2. DATA FLOW & SCOPE

Only the radiologist's dictated report text is processed. No images, orders, or patient records are accessed.

Radiologist workstation → identifier scrubbing (always on) → **TLS 1.2+** → **RadPal cloud (AES-256 at rest, US)** → **AI providers under BAA**

3. PHI HANDLING & MINIMIZATION

- **Always-on redaction.** Before any text reaches an AI provider or is stored, RadPal redacts patient identifiers: labeled patient names, dates of birth, medical record / account / accession numbers, ages 90 and over, and identifier-like tokens. This cannot be disabled by end users.
- **Defense-in-depth.** Redaction is a safeguard, not a guarantee of de-identification under 45 C.F.R. § 164.514; it operates alongside executed BAAs.
- **No training.** Clinical text is never used to train AI models.
- **Data minimization.** The application does not read or transmit images, orders, or demographics; only dictated report text is processed.

4. SUBPROCESSORS & BUSINESS ASSOCIATE AGREEMENTS

Every subprocessor that processes PHI operates under an executed Business Associate Agreement.

PROVIDER	PURPOSE	DATA HANDLING
AI language providers	AI text generation	US-based · HIPAA BAA · no model training · retention restricted by BAA (zero-retention where available) · specific vendors disclosed under NDA
Supabase (AWS, US)	Database & authentication	BAA signed · HIPAA add-on · SOC 2 Type 2
Vercel	Website hosting	No PHI processed · SOC 2 Type 2

Stripe	Payment processing	No PHI processed · PCI DSS

5. TECHNICAL SAFEGUARDS

Encryption & data protection

- TLS 1.2+ in transit; AES-256 at rest on all stored data.
- Row-level security: each user reads only their own report history.
- Point-in-time recovery, SSL enforcement, and network restrictions enabled.
- Database connection logging enabled for audit evidence.

Access control

- MFA enforced on all administrative and infrastructure accounts.
- Service-role credentials confined to server-side systems; never shipped in the client.
- AI prompt logic resolved server-side; credentials and proprietary rules never reach client devices.
- Least-privilege access, reviewed periodically.

Application security

- Signed Windows executables with verified auto-updates.
- Serverless AI proxy that persists no prompt or response content.
- Risk-minimizing releases: feature flags, kill switches, deploy-then-verify.
- PHI-path changes reviewed against an internal checklist before release.

Monitoring & response

- Immutable audit logs for PHI-relevant and security events.
- Continuous cloud security-posture monitoring with drift alerts.
- No third-party analytics, advertising, or tracking SDKs in the application.

6. GOVERNANCE & ADMINISTRATIVE SAFEGUARDS

- **Policies.** Documented Information Security Policy, Incident Response & Breach Notification Procedure, and Business Continuity / Disaster Recovery Plan, approved and reviewed at least annually.
- **Security Officer.** A designated Security Officer is accountable for security, incident response, and vendor management.
- **Workforce.** Confidentiality agreements, security-awareness training at onboarding and annually, and a disciplinary policy for violations.
- **Vendor risk.** Subprocessors are vetted for security posture and HIPAA readiness before adoption; any subprocessor handling PHI must execute a BAA.
- **Change management.** Version-controlled, deploy-then-verify releases with documented rollback.
- **Records.** Immutable audit logs; six-year retention of security and incident records.

7. INCIDENT RESPONSE & BREACH NOTIFICATION

RadPal maintains a documented incident-response procedure with defined phases (triage, containment, investigation, eradication/recovery, and post-incident review) and the HIPAA four-factor breach risk assessment. As a Business Associate, RadPal notifies affected customers of a breach of unsecured PHI without unreasonable delay and no later than 60 calendar days after discovery (internal target: five business days), consistent with the HIPAA Breach Notification Rule.

8. COMPLIANCE POSTURE

- **HIPAA.** RadPal operates as a Business Associate and executes BAAs with covered-entity customers on request, with downstream BAAs across its PHI subprocessors.
- **Infrastructure.** All infrastructure runs on SOC 2 Type 2 certified providers (Supabase / AWS, Vercel) in US regions. RadPal inherits their platform and physical controls and layers its own controls on top. RadPal itself is not separately SOC 2 audited.
- **Data residency.** All customer data is stored in AWS us-east-2 (Ohio, USA). No data is stored outside the United States.

9. WORKING WITH YOUR IT & SECURITY TEAM

- We complete vendor security questionnaires and risk assessments on request.
- We execute your institution's BAA, or provide our standard BAA for review.
- Subprocessor SOC 2 reports, our security policies, and architecture / data-flow documentation are available under NDA.
- We support your vendor-review and application allow-listing process end to end.

RadPal is a documentation productivity tool, not a diagnostic device: it does not analyze images or render diagnoses, and every output is reviewed and signed by the interpreting radiologist. This document describes RadPal's security program as of the date shown and may be updated.