Buddee Security Overview

Early-access security posture | For security review

This overview summarizes Buddee's security posture at launch stage. It describes design intent and commitments and is explicit about what is not yet independently certified. It is not a compliance certification, SOC 2 report, penetration-test report, or production customer attestation.

1. Product Safety Model

Buddee operates in shadow mode: AI surfaces suspected coding gaps and drafts, and a clinician approves, edits, or rejects every output. There is no autonomous billing or payer submission. This human-approval boundary is a core product guarantee, not a configuration option.

2. Data Protection

The application is hosted in US regions (Vercel for the app, Neon Postgres for stored data). Traffic is served over TLS, and data at rest is encrypted by our infrastructure providers. The public website and waitlist collect business contact information only; no PHI is accepted through public forms, the sandbox chat, or error reporting.

3. Access & Operational Controls

Designed controls include API-key authentication on state-changing routes, per-IP rate limiting, same-origin/CSRF checks on JSON mutations, secret management via the deployment platform, and a documented credential-rotation schedule. Tenant isolation and least-privilege access are designed for production deployments under a signed agreement.

4. Audit Trail (by design)

Buddee's audit design uses SHA-256 hash chaining so recommendation, approval, and rejection events reference the prior event hash. Durable append-only storage, verification/export tooling, and regulator-ready guarantees are on the roadmap and should not be relied upon as completed today.

5. Compliance Roadmap

Buddee signs a Business Associate Agreement before any PHI is processed. SOC 2 Type II and a third-party penetration test are planned, not yet started. An internal security review has been completed covering authentication, encryption,

access controls, and audit-logging design.

6. Review Status

This document supports early security diligence. It should be superseded by counsel-approved policies, a completed risk-assessment summary, and independent audit materials before enterprise contracting or broad paid acquisition.

Security contact: security@trybuddeeai.com | Coordinated disclosure: /.well-known/security.txt