

SECURITY AND PRIVACY POSTURE

Controls we built, and what we have **not** done.

Every row below is stated in the product's own documentation. Nothing here is a certification.

Controls in place

CONTROL	HOW IT WORKS
Tenant isolation	Row-level security is forced on every tenant-owned table; the application connects as a role that cannot bypass it. A cross-tenant id returns "not found".
Sign-in	OpenID Connect authorization code with PKCE through your identity provider. ZYVORA never sees a password. Sessions are server-side, stored hashed, 30 minutes idle and 8 hours at most.
Authorisation	Thirteen roles, deny by default, plus relationship and facility checks. A denial is itself audited. Only doctors sign notes, only pharmacists dispense, only radiologists report; a controlled drug needs a second person who is signed in as themselves.
Request integrity	CSRF double-submit on every change, a strict content-security policy, security headers and rate limits. An optional Envoy edge adds TLS and a session check.
Audit	Every read and change of a record writes an append-only, hash-chained entry in the same transaction (metadata only), with a verify endpoint.
Restricted records	Break-glass access requires a stated reason, is recorded, and is reviewed by an administrator. A privacy watch flags unusual patterns in the audit trail against rules your organisation sets; a finding names a user and a count, never a patient.
AI	Off unless an organisation enables it; private-network provider by default; identifiers removed before sending (this reduces exposure, it is not anonymisation); drafts only; a named human review, bound to the clinician's own note revision for note drafts.

What is not done

Certification	Not certified or attested against HIPAA, GDPR, ISO 27001, SOC 2, IEC 62304, NABH/JCI or similar. A gap list is published.
Independent review	No independent penetration test. The audit trail is tamper-evident, not tamper-proof against a database owner.
Clinical validation	No model has been clinically validated. Drug-interaction and dose checks report "unavailable" without a drug database.
Privacy workflows	No automated retention or erasure workflows yet; the privacy impact assessment lists what the operator must define.
Testing gaps	No load testing, no screen-reader testing, Chrome only for browser tests. An automated accessibility audit passes but is not a conformance claim.

Contact for security questions: security@zyvor.dev. Vulnerabilities are reported privately, not in public issues.