

VIBE96 QUALITY REPORT

ClinVexa

Self-hosted clinic management system for patients, queue, EMR, pharmacy, lab and billing, in English, Bangla and Arabic.

Product ID	**B0555-98379**
Builder	**MST RATNA BEGUM**
Version reviewed	**1.0.0 · released 27 Nov 2026**
Stack	**Next.js 15.5.29 (App Router) + React 19.1.10 · TypeScript 5.9 on Node.js 22.12+ · PostgreSQL 16 (postgres:16-alpine image) via Prisma 6.19.3**
Built with	**Claude Code**
Review period	**18 Nov 2026 – 27 Nov 2026 · 1 round of changes**

76 / 100

Passed with 5 warnings

Pass mark 75 and no failing check.

Scores

Security	79
Code structure	88
Docs & completeness	80
Dependency health	60
Build & deploy	72

✓ **AI code audit**
6 checks · 15 Nov 2026

✓ **Installed & run**
26 Nov 2026

✓ **Demo vs delivered**
27 Nov 2026

✓ **Final sign-off**
27 Nov 2026

At a glance

- ✓ Installed and run from the delivered code — 8 of 8 checks answered yes.
- ✓ Live demo compared with the delivered code — 7 of 7 checks answered yes.
- ! 12 of 15 promised items delivered (setup guide, example config and the rest).
- ✓ Security scored 79/100 with no failing check.
- ! 5 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00158. The online copy always shows the latest status.

PART 1

AI code audit

The full source archive was read by our AI auditor against each check. It reads the code — it does not run it; running it is part 2.

CHECK	WHAT WE FOUND	SCORE	RESULT
Secrets & credentials	All regex candidates are placeholders, env-var references, schema definitions or unit-test constants; no live keys, committed .env files or connection strings with real credentials were found. The only concern is that the README publishes demo account passwords that seed.sql creates, so a buyer who loads the seed and forgets to change them would have a known admin login.	88	Warning
Dependency vulnerabilities	The only manifest is Node a project file. No package-lock.json is in the tree (the file listing omits lockfiles, so this needs confirming), and every dependency uses a caret range, so installs are not reproducible. The declared versions (Next 15.5.x, React 19, Prisma 6, Zod 3) are recent and have no known critical vulnerabilities, but a few ESLint, Vitest and Prisma ranges need attention.	60	Warning
Authorisation & access control	The documented design wraps every handler in api('<permission>'), checks same-origin, reloads the user from the DB and uses bcrypt hashing with signed JWT sessions. However, none of the ~35 route files or the services were included in the excerpts, so guards on each mutating endpoint and ownership checks on id lookups are unverified. Middleware only checks token validity and excludes /api, so all API protection depends on the wrapper being applied everywhere.	72	Warning
Database access rules	The project accesses data via Prisma with Zod-validated input and documents scoped, soft-delete patterns, so no injection path or unscoped destructive statement is visible in the supplied excerpts. However, most service files, the full schema and the SQL scripts were not provided, so completeness, foreign-key indexes and N+1 behaviour could not be fully verified. Visible gaps are missing indexes on several foreign keys and an unclear relation between the Prisma schema and the hand-maintained SQL.	78	Warning
Code structure & duplication	The project follows a documented strict layering (routes thin, services hold business logic, validators separate, one panel per module), which the file tree supports. Only the excerpts were available, so file lengths and duplication inside the omitted components could not be measured directly.	88	Pass
Build reproducibility	Manifests, Dockerfile and compose are coherent, and referenced folders exist. However no lockfile is shipped, the Docker build depends on a NEXT_STANDALONE flag not visible in the digest, and the setup order and prerequisites could not be fully verified from HowToSetup.md.	72	Warning

Open warnings

Problems that did not stop the listing. They stay on the product page until a later version fixes them.

Warning 1 **No real credentials found; demo logins and seed data ship known weak passwords**

All regex candidates are placeholders, env-var references, schema definitions or unit-test constants; no live keys, committed .env files or connection strings with real credentials were found. The only concern is that the README publishes demo account passwords that seed.sql creates, so a buyer who loads the seed and forgets to change them would have a known admin login.

Warning 2 **No lockfile shipped; caret ranges only; dependency versions look current with no known critical CVEs**

The only manifest is Node a project file. No package-lock.json is in the tree (the file listing omits lockfiles, so this needs confirming), and every dependency uses a caret range, so installs are not reproducible. The declared versions (Next 15.5.x, React 19, Prisma 6, Zod 3) are recent and have no known critical vulnerabilities, but a few ESLint, Vitest and Prisma ranges need attention.

Warning 3 **Mostly reproducible; lockfile absent, config split across two env files, setup doc unverified**

Manifests, Dockerfile and compose are coherent, and referenced folders exist. However no lockfile is shipped, the Docker build depends on a NEXT_STANDALONE flag not visible in the digest, and the setup order and prerequisites could not be fully verified from HowToSetup.md.

Warning 4 **Prisma-only access with scoped deletes; schema partly unverified and has FK index gaps**

The project accesses data via Prisma with Zod-validated input and documents scoped, soft-delete patterns, so no injection path or unscoped destructive statement is visible in the supplied excerpts. However, most service files, the full schema and the SQL scripts were not provided, so completeness, foreign-key indexes and N+1 behaviour could not be fully verified. Visible gaps are missing indexes on several foreign keys and an unclear relation between the Prisma schema and the hand-maintained SQL.

Warning 5 **Auth design looks sound, but route handlers were not visible so per-route guards and ownership cannot be verified**

The documented design wraps every handler in api('<permission>'), checks same-origin, reloads the user from the DB and uses bcrypt hashing with signed JWT sessions. However, none of the ~35 route files or the services were included in the excerpts, so guards on each mutating endpoint and ownership checks on id lookups are unverified. Middleware only checks token validity and excludes /api, so all API protection depends on the wrapper being applied everywhere.

Requirement list

What the builder agreed to deliver before uploading — 12 of 15 met.

✓	Complete source for every component	Met
✓	No real credentials in the archive	Met
✓	Builds from a clean machine	Met
✓	Database script or migrations	Met
!	Authentication and roles on every mutating endpoint	Partial
!	Pinned dependencies without critical CVEs (nice)	Partial
✓	Documentation set (nice)	Met
!	Working live demo	Partial
✓	README.md	Met
✓	HowToSetup.md	Met
✓	CLAUDE.md (or AGENTS.md) (nice)	Met
✓	CHANGELOG.md (nice)	Met
✓	.env.example	Met
✓	a project file	Met
✓	a project file (nice)	Met

PART 2

Human review

Reviewers from the Vibe96 team in Dubai worked through each question below; a final reviewer signed it off.

Stage 1 — Installed and run from the delivered code

Completed 26 Nov 2026

A reviewer installed the product on a clean machine, following only the guide that ships with it.

QUESTION	ANSWER	REVIEWER'S NOTE
Packages restored without errors	Yes	
Solution builds clean	Yes	
Database created from the shipped script or migrations	Yes	
First sign-in works with the documented steps	Yes	
Setup guide is accurate and complete	Yes	
Every module in the feature list opens and works	Yes	
No real secrets in the archive	Yes	
Branding and company details can be changed without code	Yes	

Stage 2 — Live demo compared with the delivered code

Completed 27 Nov 2026

A second reviewer checked that what the listing and demo show is what the buyer receives.

QUESTION	ANSWER	REVIEWER'S NOTE
Demo URL is reachable	Yes	
Demo credentials work	Yes	
Demo runs the same version as the archive	Yes	
All five differentiators are visible in the demo	Yes	
Screenshots match the demo	Yes	
Nothing in the demo is missing from the code	Yes	
Datasheet claims are accurate	Yes	

Changes asked for during review

None — approved on the first round.

Sign-off: approved for sale on 27 Nov 2026 with 5 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.0.0 exactly as the buyer downloads it: the source archive, the setup guide and the live demo on the dates above.

- **It is not** a penetration test, a performance or load test, or a legal review of third-party package licences.
- **Scores are a point in time.** Libraries age; a later version is audited again and gets its own report.
- **Your setup matters.** Hosting, configuration and changes made after purchase are outside this review.
- **How the score is made:** each AI check is scored 0–100 and weighted (security counts most). A listing needs 75 or more, no failing check, and the human review passed.
- **Always try the live demo** before buying, and ask the builder questions from the product page.