Security & Data Privacy Summary

What GritLeanPulse does to protect clinic and patient data

For IT and compliance review — GritLeanPulse — SJK & Sons LLC

Encryption & Infrastructure

- All data is encrypted at rest (AES-256) and in transit (TLS/HTTPS).
- Hosted on Supabase, running on SOC 2-compliant cloud infrastructure.
- Regular security reviews and access-control audits as part of standard operations.

Access Control

- Row-Level Security (RLS) is enabled on every database table without exception — a user's data is isolated at the database layer itself, not only in application code. Even a bug in the application cannot expose another user's records; the database refuses the query.
- Clinic Portal staff PINs are hashed with scrypt (a memory-hard, brute-force-resistant algorithm) with a unique random salt per account — never stored or transmitted in plaintext.
- Clinic Portal sessions are signed tokens that expire automatically after 12 hours.
- The elevated database credentials capable of bypassing row-level security are never exposed to a browser or mobile app — they exist only inside server-side code.

What Your Practice Can and Cannot See

Your practice does not have standing access to a patient's full health record. A patient's account is private to them by default. The only information your organization ever sees is what a patient actively chooses to share — a message they send through Provider Messaging, or a Progress Report they tap to send before an appointment — filtered through the specific data categories that patient has consented to share, enforced on the server before any data is returned.

Data Use

- GritLeanPulse never sells or rents patient data to any third party, for any reason.
- Data is disclosed only: as required by law, as directed by the clinic partner regarding their own patients, or to necessary sub-processors (cloud hosting and database infrastructure) required to operate the service.

Regulatory Status

GritLeanPulse is a consumer wellness application — not a healthcare provider, health plan, or clearinghouse — and does not claim HIPAA certification. We would rather state that plainly than have any partner assume otherwise. The technical safeguards described above are real and implemented independent of that distinction.

If your organization's internal policy requires a signed Business Associate Agreement regardless of technical applicability, contact us directly — we are glad to discuss this on a case-by-case basis for qualifying partners.

Questions

Suzanne Evans, Founder — SJK & Sons LLC | suzanne.evans@gritleanpulse.com | gritleanpulse.com