Security and privacy assessment

Controls in release 1.0, known gaps and what must be in place before real patient data is entered. Not legal advice.

1. Summary

Release 1.0 keeps all patient data encrypted in the user's browser and sends nothing to a server. That removes server-side attack surface but puts the weight on the device, the sign-in and the backup routine. It is suitable for synthetic data, pilots and single-user clinical work on a managed device. Multi-user clinical production needs the server edition.

2. Controls in place

Area	Control
Authentication	Password checked against a salted PBKDF2-SHA256 hash (310,000 rounds); optional authenticator app (TOTP) with recovery codes; lockout after repeated failures; automatic lock after 15 minutes idle.
Encryption at rest	AES-GCM vault; key derived from the password and never stored.
Encryption in transit	Not applicable to patient data (none is transmitted). The page itself must be served over HTTPS.
Content security	Strict Content-Security-Policy: no external scripts; network requests limited to the same site.
Roles	Clinician, data manager, administrator, researcher. Researcher is read-only, sees no names or dates of birth, gets de-identified exports only and masked small counts.
Audit	Every create, change, state change, extraction review, ranking run and export is logged with time, role and user.
Data minimisation	Optional fields for gender identity and ancestry; research exports drop names, dates of birth, contacts, clinician names and free text.
Pseudonymisation	Random research key per patient, unrelated to the patient ID.
Consent	Recorded per purpose; withdrawal blocks research exports.
Integrity	Verified records are locked; changes need an amendment with a reason.

3. Known gaps and risks

Risk	Effect	Mitigation

One shared sign-in	Roles are a working mode, not separate accounts; the audit trail records the name typed in settings.	Use on a personal managed device; move to the server edition for teams.
Data lives in one browser	Clearing site data or losing the device loses the data.	Export a backup after each session to approved secure storage; the backup file is not encrypted.
Backup file is plain JSON	Anyone with the file can read it.	Store only on encrypted, access-controlled storage; never email.
Malware or shared device	An unlocked session exposes data.	Managed device, screen lock, authenticator app enabled.
Free-text notes	May contain identifiers that structured de-identification misses.	Free text is left out of research exports.
Re-identification from rare phenotypes	A rare combination of findings can identify a person even without a name.	Minimum cell size on counts; governance review before any external sharing.
Decision support	Ranking or extraction could be over-trusted.	Labelled as research-use; human acceptance required; not a diagnosis.

4. Legal and governance points to settle

- EU GDPR: genetic and health data are special-category data. A lawful basis and an Article 9 condition are needed, with a data-protection impact assessment, records of processing, and processor agreements with any host.
- India Digital Personal Data Protection Act 2023: consent notice, purpose limitation, rights of the data principal, breach notification and rules for children’s data apply. Check the current rules and notifications with counsel.
- Cross-border transfer between the EU and India needs a transfer mechanism.
- Ethics approval for research use; institutional policy on retention and deletion.
- If any output is used to diagnose or guide treatment, assess whether the software is a medical device under the applicable regulation.

5. Requirements for the server edition

- Individual accounts with single sign-on and enforced two-factor authentication; role-based access on every API route.
- TLS everywhere; database and object-storage encryption; secrets in a managed vault; separate development, test and production environments.
- Append-only audit log; export approval workflow; automated daily backups with a tested restore.
- Clinical data and large genomic files in separate stores; only metadata, checksums and access policy in the database.
- Penetration test and dependency scanning before go-live.

6. Before entering real patient data

- ☐ Privacy and ethics review completed and documented.
- ☐ Device is managed, encrypted and has a screen lock.

- ☐ Authenticator app enabled; password changed from the initial one.
- ☐ Backup location approved; restore tested once.
- ☐ Consent forms reviewed by counsel and in use.
- ☐ Staff know that ranking and extraction are aids, not diagnoses.

© Tribro-Omics · Security and privacy assessment · Version 1.0 · 11 November 2026