Security audit — CRM V11 and TribroLIMS V5

Control-by-control review with evidence, cryptography inventory, findings and actions. Technical audit by the developer of the build; not an independent or legal assessment.

1. Scope and method

Scope: Tribro-Omics CRM V11 and TribroLIMS V5 as single-file browser applications, their sign-in, storage, backup, audit trail, report sign-off and the CRM ↔ LIMS link. Method: review of the code paths and the automated tests listed in the test report (same date). Evidence references (SEC, LNK, NEG) point to that report.

2. Conclusion

The controls that can exist in a browser-only application are in place and behaved as designed in every test: 99 of 99 security and link checks passed. The two largest remaining risks are structural, not defects: the initial password is still in use (F1), and nothing is enforced by a server (F2). Twelve findings are listed in section 6: 2 high, 5 medium, 4 low, 1 informational.

3. Controls

Control	How it works	Evidence	Assessment	Residual risk
Sign-in	User name and password checked against a salted PBKDF2-SHA256 hash (310,000 rounds); constant-time comparison.	Wrong password refused; no data readable without it.	Effective	Depends on password strength; the hash is inside the public file.
Two-step sign-in	TOTP (RFC 6238), required by policy; 8 one-time recovery codes; a code cannot be used twice.	SEC tests “password alone does not open the app”, “wrong sign-in code refused”, “correct code signs in”, in both applications.	Effective	Checked in the browser, see finding F2.
Step-up for sensitive actions	Authenticator code asked again for sign-off, backup export, case deletion, identifiable cohort export, link code change, switching the policy off.	LNK-n.08 and LNK-n.09 in all five rounds; backup and link-code tests.	Effective	None beyond F2.

Lock-out	Increasing delay after five wrong passwords.	Earlier build tests; failed attempts are shown in “Recent sign-ins”.	Effective	Counter is stored in the browser and can be cleared by someone with device access.
Idle lock	Automatic lock after 5–30 minutes (default 15).	Configuration test; behaviour unchanged from earlier builds.	Effective	A 30-minute setting weakens it.
Encryption at rest	All data in one AES-256-GCM vault; key derived from the password, never stored.	Storage inspected after use: no readable case data.	Effective	Unlocked session exposes data in memory.
Encrypted backup	AES-256-GCM with a separate passphrase; plain export removed.	Backup file contains no readable data; wrong passphrase refused; restore works.	Effective	Passphrase loss makes the backup useless.
Audit trail integrity	Each entry stores SHA-256 of the previous entry and its own content.	Chain verifies; an edited entry is detected; chains still valid after five link rounds.	Effective against casual change	See finding F9.
Report integrity	SHA-256 fingerprint at sign-off; released reports locked; amendments are new versions.	Fingerprint verified; altered text detected (V3 workflow test).	Effective	None.
Link confidentiality and integrity	AES-256-GCM with a key from the shared link code; message type and sender bound into the encryption; delivery receipts.	Wrong link code, altered package and unknown case all refused; mailbox contains no readable data.	Effective	See finding F5.
Role restrictions	Five laboratory roles limit actions; researcher mode in the phenotype module is read-only and de-identified.	Technician cannot sign (V3 workflow test).	Partly effective	See finding F3.
Browser hardening	Content-Security-Policy; no third-party scripts; refuses to run inside a frame.	Present in both builds.	Effective	Fonts are loaded from Google, see F10.
Consent enforcement	Research exports blocked when research consent is declined or withdrawn.	Phenotype module tests.	Effective	None.

4. Cryptography in use

Purpose	Algorithm	Key or parameters
Password check	PBKDF2-HMAC-SHA256	310,000 rounds, 16-byte random salt, 256-bit output
Data vault	AES-256-GCM	Key from the password (PBKDF2, own salt); 12-byte random IV per save

Encrypted backup	AES-256-GCM	Key from the backup passphrase (PBKDF2, 310,000 rounds, random salt)
Link packages	AES-256-GCM with associated data (type and sender)	Key from the link code (PBKDF2, 200,000 rounds, fixed application salt)
Two-step codes	TOTP, HMAC-SHA1, 6 digits, 30 s	160-bit random secret kept in the vault; ±1 step tolerance; no re-use
Recovery codes	SHA-256 of each code	8 codes of 10 characters, single use
Audit chain, report fingerprint	SHA-256	Chain over previous hash and entry content; fingerprint over report content
Random values	Browser cryptographic generator	Salts, IVs, secrets, identifiers

All primitives come from the browser's Web Crypto interface except the synchronous SHA-256 used for the audit chain, which was compared with a reference implementation on seven inputs.

5. Data flow of the link

- CRM → LIMS "case": the full case record (identifying data, phenotype, pedigree, consent) and an optional test request.
- LIMS → CRM "result": order number and state, sample numbers and states, and for a released report the result, summary, interpretation, classified variants, signer and fingerprint.
- Each package is encrypted before it is written to browser storage and is removed when imported or rejected. The sender receives "Delivered" or "Refused" with the reason.
- Connection tests and receipts are handled automatically; cases and results are imported only when the user presses Import.
- For a second device the same encrypted package is saved as a file. It contains no readable data.

6. Findings

No.	Severity	Finding	Effect	Recommended action
F1	High	The initial password is the same in the CRM, TribroLIMS and TribroPheno, and its hash is inside the downloadable files.	Anyone who obtains the initial password can open a fresh copy of each application; a weak password could be guessed offline.	Change the password in every application at first use to a long passphrase (20+ characters), different per application. The security check flags this until done.
F2	High	All checks run in the browser. There is no server that enforces them.	Someone who can change the files on the server, or who uses an unlocked device, can bypass sign-in logic for new data or read data in memory. Existing data stays encrypted without the password.	Restrict hosting (FTP) access, enforce HTTPS and the delivered headers, use managed devices with screen lock. For a team, plan the server edition.

F3	Medium	One sign-in per application; staff roles are not separate credentials.	The audit trail records the selected operator, which a signed-in user could switch.	Use one device profile per person where possible; sign-off already needs password and authenticator. Individual accounts need the server edition.
F4	Medium	The applications share the web origin tribro-omics.com with the public website.	A script flaw on any public page (for example the chatbot page) could read or delete the encrypted vaults and the link mailbox. It could not decrypt them, but it could destroy data or show a false sign-in page.	Move the CRM and TribroLIMS to their own sub-domain (for example lab.tribro-omics.com) so that browser storage is isolated from the public site.
F5	Medium	The link uses a shared code kept in both vaults; packages wait in browser storage.	A weak or leaked link code would let someone with access to the browser profile read waiting packages.	Use the generated 15-character code or longer; change it if a device is lost; import packages promptly.
F6	Medium	TribroLIMS/demo.html (the earlier tour) shows its own demo password and stores settings unencrypted.	It holds only demonstration data, but it looks like a sign-in and may confuse users or auditors.	Remove demo.html from the production server, or keep it only on a separate demonstration address.
F7	Medium	All data lives in one browser on one device.	Clearing browser data or losing the device loses everything since the last backup.	Create an encrypted backup after every session; store it on approved secure storage; test a restore.
F8	Low	Unencrypted backup files from older versions can still be imported.	An old plain file could be restored by mistake and such files may exist on disk.	Delete old plain backup files after making an encrypted one.
F9	Low	The audit chain is kept inside the same vault as the data.	A person with the password and technical skill could rebuild the chain after a change.	Download the audit CSV and the security report regularly to independent storage; the hashes then act as an external anchor.
F10	Low	Fonts are loaded from Google Fonts.	Each page load tells Google the user’s IP address, which matters under the GDPR.	Host the three fonts on tribro-omics.com.
F11	Low	Two-step sign-in can be switched to “optional” by a signed-in user (after an authenticator code).	The policy depends on the user keeping it on.	Leave it on “Required”; the security check shows the state.
F12	Info	Not verified in this audit: live HTTPS configuration on STRATO, a penetration test, a physical authenticator app, legal review.	—	Check the response headers after upload; commission a penetration test before clinical use.

7. What the audit trails record

- Phenotype module: case created, opened, every field change, observation and annotation changes, extraction runs and reviews, ranking runs, state changes, amendments with reason, every export, link transfers.
- Laboratory: order, sample registration, accessioning or rejection, each extraction and library attempt and its QC decision, run changes, analysis, VCF imports, each classification with criteria, report draft, review, sign-off (with the factors used), fingerprint checks, exports, operator switches, threshold and policy changes.
- Security: sign-ins with two-step flag and failed attempts before them; backups; policy and link-code changes.
- Each entry: time, operator, role, action, record, detail, and the chain hash.

8. Data-protection pointers (not legal advice)

- Genetic and health data are special-category data under the GDPR and sensitive under India’s Digital Personal Data Protection Act. A data-protection impact assessment and a documented lawful basis are needed before real patient data is entered.
- Record where backups are stored and who can reach them.
- Finding F10 (Google Fonts) and finding F4 (shared origin) should be closed before go-live.

9. Actions before real patient data

- ☐ Change the password in the CRM, TribroLIMS and TribroPheno (F1).
- ☐ Set up the authenticator in each application and store the recovery codes.
- ☐ Move the applications to their own sub-domain (F4) and confirm HTTPS and headers (F12).
- ☐ Remove demo.html from production (F6) and remove the demonstration data in TribroLIMS.
- ☐ Agree the backup routine and test one restore (F7).
- ☐ Host fonts locally (F10).
- ☐ Complete privacy, ethics and quality-system validation.

© Tribro-Omics · Security audit — CRM V11 and TribroLIMS V5 · Version 1.0 · 12 November 2026