

Testing checklist: clinical trial management software

Source: <https://howtotestaproduct.com/how-to-test/clinical-trial-software/>

Generated: 2026-10-07. Licence: CC BY 4.0.

☐ 1. release smoke tests

Done when: After each deployment to production, a test site enters, edits and signs one eCRF page, and the audit trail shows the old value, new value, user, time and reason.

Risks: data-corruption, regulatory-penalty. Tool class: browser automation. Usually run by: QA engineer.

☐ 2. penetration testing

Done when: A blinded site user and a sponsor monitor each try to read the treatment arm or another site's participants by changing ids, and both attempts fail.

Risks: data-breach, user-harm. Tool class: proxy. Usually run by: security specialist.

☐ 3. unit tests

Done when: Every combination of randomisation strata allocates from the expected table, and dose calculations match the protocol table at each weight boundary.

Risks: user-harm. Tool class: unit framework. Usually run by: developer.

☐ 4. end-to-end functional tests

Done when: A test participant is screened, randomised, assigned a kit and emergency-unblinded by the investigator, and only the investigator and named unblinded roles see the arm.

Risks: user-harm. Tool class: browser automation. Usually run by: QA engineer.

☐ 5. regression suite

Done when: Before each release, the validated scripts for edit checks, signatures and audit trail rerun and pass on the release candidate, and the result is filed in the validation package.

Risks: regulatory-penalty, data-corruption. Tool class: browser automation. Usually run by: QA engineer.

☐ 6. data integrity and migration testing

Done when: After a protocol-amendment migration, a reconciliation report shows every subject, visit and value matches the pre-migration export, and audit trails are carried over unchanged.

Risks: data-corruption, regulatory-penalty. Tool class: data validation. Usually run by: QA engineer.

☐ 7. compliance checks

Done when: A signed validation package maps each Part 11 and GCP requirement (audit trail, e-signature, access control, retention) to a test record an inspector can open.

Risks: regulatory-penalty. Tool class: test management. Usually run by: QA engineer.

☐ 8. integration tests

Done when: Lab, eCOA and device files imported into the EDC land on the right subject and visit, with the same values and units as the source file.

Risks: data-corruption. Tool class: API client. Usually run by: developer.

☐ 9. security scanning

Done when: The scan report for the EDC and its export endpoints shows no open high-severity finding, and a deactivated site user cannot sign in.

Risks: data-breach. Tool class: DAST scanner. Usually run by: security specialist.

☐ 10. resilience and failure testing

Done when: With the randomisation service switched off in staging, the site follows the documented fallback, and entries made during the outage appear with correct timestamps after recovery.

Risks: dependency-failure. Tool class: chaos tool. Usually run by: developer.