

Testing checklist: patient portal

Source: <https://howtotestaproduct.com/how-to-test/patient-portal/>

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

☐ 1. release smoke tests

Done when: After each release, a test patient signs in, views a test result, sends a message and sees it arrive in the test clinician's inbox.

Risks: lost-actions. Tool class: browser automation. Usually run by: QA engineer.

☐ 2. end-to-end functional tests

Done when: A records request, a secure message and a proxy invitation each reach the right staff queue or account, and a revoked proxy can no longer open the patient's results.

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

☐ 3. analytics and event tracking tests

Done when: A network capture of sign-in, results, messages and appointment pages shows no request to an advertising or analytics domain carrying a name, result, page path or signed-in flag.

Risks: data-breach, regulatory-penalty. Tool class: proxy. Usually run by: QA engineer.

☐ 4. accessibility testing

Done when: A screen reader user signs in, reads a lab result, books an appointment and sends a message without sighted help.

Risks: accessibility-liability. Tool class: accessibility checker. Usually run by: accessibility specialist.

☐ 5. compliance checks

Done when: A reviewer confirms that a records request made through the portal is logged with a due date and that a test patient can download their record in a standard format.

Risks: regulatory-penalty. Tool class: test management. Usually run by: product manager.

☐ 6. security scanning

Done when: The scan report for the portal web app, mobile apps and API lists no open high-severity finding that exposes results, messages or proxy documents on the release date.

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

☐ 7. penetration testing

Done when: A tester signed in as one patient or proxy cannot open another patient's results, messages or documents by changing an ID or replaying a link.

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

☐ 8. integration tests

Done when: Every message type sent from the portal appears in the EHR inbox for the right care team and is filed to the patient's chart.

Risks: lost-actions. Tool class: API client. Usually run by: developer.