

Testing checklist: mental health app

Source: <https://howtotestaproduct.com/how-to-test/mental-health-app/>

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

☐ 1. release smoke tests

Done when: On the release build, a test user completes onboarding, logs a mood entry and opens a therapy session screen on the oldest supported phone.

Risks: store-rejection. Tool class: mobile automation. Usually run by: QA engineer.

☐ 2. end-to-end functional tests

Done when: A test user signs up, gives or refuses consent, books a session and cancels the subscription, and each choice shows in the account settings afterwards.

Risks: money-loss, regulatory-penalty. Tool class: mobile automation. Usually run by: QA engineer.

☐ 3. payment and money-flow testing

Done when: After a test user cancels in the app, the store or payment sandbox shows the subscription ended and no charge on the next renewal date.

Risks: money-loss. Tool class: API client. Usually run by: QA engineer.

☐ 4. compliance checks

Done when: A reviewer confirms the consent screen names every third party that receives health data, the age gate blocks under-age sign-up without parental consent, and the store health declarations match the build.

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

☐ 5. analytics and event tracking tests

Done when: A network capture of onboarding, mood logging and session booking shows no questionnaire answer, mood value or condition name sent to any advertising or analytics domain.

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

☐ 6. security scanning

Done when: The scan report for the app and API lists no open high-severity finding on the release date, and no journal or chat text is stored unencrypted on the phone.

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

☐ 7. penetration testing

Done when: A tester signed in as one user cannot read another user's journal, chat or intake answers by changing an ID in a request.

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