

Trust needs answers.

Review how access is controlled, what information is shared, and who is responsible for follow-up before introducing Moonbridge to patients.

01 Protected sign-in

Passkeys and verified second-factor sign-in support account protection. Staff use individual accounts with permissions tied to their roles.

02 Care-based access

Clinical access follows authorized care relationships. No staff member can open companion conversations, whatever their license or role.

03 Recorded decisions

Sharing, corrections, and plan approvals retain a record of what was accepted and by whom. Corrections link to prior versions rather than silently rewriting signed history.

04 Clinician control

The clinician reviews concerns and approves clinical plans. A clinical pause can stop companion conversation without waiting for an urgent safety flag.

Agree on the practical details

Review hosting and encryption, service-provider terms, retention, records access, and your practice's responsible clinician and coverage arrangements. The security review should match the service you will actually use.

Know where to turn for urgent help.

Moonbridge is not continuously monitored. Do not wait for an app reply in an emergency. In the U.S., call or text 988 for crisis support; call 911 for immediate danger.

This overview describes the service controls. It is not a security certification or a guarantee that every risk can be prevented.