



Therapist Genie® · Version October 2026

Security overview for IT reviewers

Therapist Genie runs inside Microsoft 365 and Microsoft Azure. This overview separates the controls a practice inherits from Microsoft from the ones Therapist Genie designed, sets out how each kind of data is held, and answers the first questions reviewers ask. For a full questionnaire, email security@therapistgenie.com.

Inherited from Microsoft 365 and Azure

- Services audited under SOC 2 and certified to ISO/IEC 27001: Microsoft's, not Therapist Genie's
- HIPAA-eligible cloud services
- Encryption at rest and in transit
- Multi-factor authentication and conditional access (Microsoft Entra ID)

Designed by Therapist Genie

Identity

Individually identified, role-scoped accounts, and staff passwords that stay with Microsoft.

Data

Audit trails, seven-year retention, and recordings and transcripts held inside the platform rather than on personal devices or third-party services.

AI

Protected health information (PHI) is scrubbed, client data is never used to train AI models, ours or anyone else's, the reasoning behind a draft can be opened, and nothing enters a chart until a clinician signs it.

Clinical governance

Explicit signature authority, withdrawals recorded as their own events, renewals raised before they lapse, date-bounded chart sharing, signed notes that lock, and location of service on every note.

How each kind of data is held

Data	Where it is held	Retention and records
Clinical record: charts, notes, assessments and consents	Inside the platform, on Microsoft 365 and Azure services.	Seven-year retention and an audit trail. Signed notes lock; a clinician signs every note.
Session recordings and transcripts	Inside the platform, not on personal devices or third-party services.	Seven-year retention.
Back-office files: policies, credentialing files, provider identifiers, contracts, training	The practice's own Microsoft 365 storage.	Organized, permissioned, retained and searchable in Microsoft 365, under the practice's own settings.
Staff sign-in	Microsoft Entra ID. Therapist Genie does not store staff passwords.	Multi-factor authentication and conditional access, set by the practice. Every person has their own login, scoped to their role.
Client information in AI features	Processed inside the platform; protected health information (PHI) is scrubbed.	Never used to train AI models, Therapist Genie's or anyone else's. The reasoning behind a draft can be opened, and nothing enters a chart until a clinician signs it.

Questions reviewers ask

Do you have SOC 2 or ISO 27001 of your own?

No. Therapist Genie builds on Microsoft 365 and Azure services that are audited under SOC 2 (an attestation report), certified to ISO/IEC 27001 and HIPAA-eligible, and a practice inherits that control environment. Those audit reports and certifications belong to Microsoft's services, not to Therapist Genie.

Do you sign a business associate agreement?

Yes, Therapist Genie signs a business associate agreement (BAA) with customers. Ask us how it applies to your practice.

Which Microsoft 365 plan does a practice need?

A basic Microsoft 365 plan is enough, licensed from Microsoft. Sessions run in Microsoft Teams and scheduling in Microsoft Outlook. Microsoft 365 Copilot is optional, and licensed from Microsoft.

What happens when a staff member or contractor leaves?

Access comes from the same Microsoft identity as the record, so removing the person in Microsoft 365 ends their access to the record, the files and the team channels at once.

Contacts

Security questions and reports: security@therapistgenie.com

Privacy: privacy@therapistgenie.com

Everything else: info@therapistgenie.com

2563 S. Val Vista Dr. Suite 108, Gilbert, AZ 85295

Version October 2026. Microsoft, Microsoft 365, Azure, Teams, Outlook, Entra ID and Copilot are trademarks of the Microsoft group of companies.