

PRIVACY POLICY & DATA SECURITY STATEMENT

How we handle *your data*.

Last updated: August 2, 2026 · Version 2.1 · Rewire App LLC

OVERVIEW

Our commitment to data protection

Rewire is operated by Rewire App LLC ("Rewire", "we", "us"). We provide a practitioner-assigned between-session support tool for use in conjunction with qualified mental health therapy. Because our platform is used in a clinical context, we treat data protection as a clinical governance obligation.

This policy applies to all users of the Rewire platform: licensed practitioners ("Providers") and their clients ("End Users") who access Rewire under a practitioner's assignment.

For clinical governance review: Rewire is not a HIPAA Covered Entity under 45 CFR §160.103. However, we are actively building our security controls toward HIPAA's Technical Safeguard requirements (45 CFR §164.312) — including access controls, audit logging, and encryption in transit — and can discuss a Business Associate Agreement (BAA) with US-based healthcare providers upon request. We are committed to full GDPR compliance for all European users under Regulation (EU) 2016/679. Our primary data processor, Supabase, maintains SOC 2 Type II certification and operates GDPR-compliant infrastructure. Data transfers to the US are governed by Standard Contractual Clauses (SCCs).

01 — DATA CONTROLLER

Who is responsible for your data

Data Controller: Rewire App LLC

For all data protection enquiries, data subject rights requests, and Business Associate Agreement requests:

Email: privacy@rewire-emdr.com

Subject line: "Data Privacy Request"

We will acknowledge all requests within 72 hours and respond in full within 30 days.

02 — DATA WE COLLECT

What we collect and why

rewire-emdr.com/privacy · Version 2.1 · Effective August 2, 2026 · Downloaded copy — current terms at rewire-emdr.com/privacy

Practitioner (Provider) accounts

DATA TYPE	PURPOSE	LEGAL BASIS (GDPR)
Email address	Account authentication and platform communications	Contract performance — Art. 6(1)(b)
Practice name	Displayed within the provider dashboard; identifies the practice to their assigned clients	Contract performance — Art. 6(1)(b)
Subscription and billing data	Payment processing via Stripe. Card details are not stored by Rewire. Stripe is PCI DSS Level 1 compliant.	Contract performance — Art. 6(1)(b)
Client roster and account details	Client account identifiers, email addresses, optional first names, practitioner and facility links, and access or invitation codes used to provide and administer care access.	Contract performance — Art. 6(1)(b)

End User (client) data

DATA TYPE	PURPOSE	LEGAL BASIS (GDPR)
Email address	Authentication and service communications. Shared with service providers such as Supabase, Resend, and Stripe only as needed to operate the service; not sold or shared for advertising.	Contract performance — Art. 6(1)(b)
Session completion data	Records which exercises have been completed. Visible to assigning practitioner.	Legitimate interests — Art. 6(1)(f) (clinical care continuity)
Nervous system state ratings	Pre/post exercise ratings (0–10 scale) entered by the user. Shared with assigning practitioner for clinical review.	Consent — Art. 6(1)(a)
Journal entries	Optional written reflections entered during exercises. Shared with the assigning practitioner only if the user explicitly enables sharing. Constitutes potentially special category data.	Explicit consent — Art. 9(2)(a)
AI conversation transcripts	Used in real time to generate personalised session content only. Not stored permanently. Not used for AI model training.	Consent — Art. 6(1)(a)

Data we do not collect

- Rewire does not require a full legal name for an individual client account, but may collect an optional first name and practitioner or facility rosters may include identifying account details
- Rewire does not require a structured clinical diagnosis or mental health history for client signup; users and practitioners may nevertheless enter health information in free-text clinical fields
- User data is not sold, licensed, or shared with third parties for commercial purposes
- No user data — including AI conversations — is used to train AI models

03 — DATA STORAGE & SECURITY

How we protect your data

Infrastructure

User data is stored primarily in **Supabase**, a managed PostgreSQL-based platform. Data is stored on managed infrastructure that provides encryption at rest. Application traffic to Rewire's service providers is encrypted in transit using HTTPS/TLS. Security certifications and infrastructure controls are maintained by the relevant service providers.

Access controls and row-level security

Rewire implements row-level security (RLS) at the database layer. Each practitioner can access only the session data for clients they have directly assigned using their own practitioner access code. No practitioner can access data belonging to clients of a different practitioner. No Rewire employee accesses user session data or journal entries in the ordinary course of operations.

AI processing safeguards

AI-generated content is routed through a Cloudflare Worker to a secure, HIPAA-covered third-party AI provider. Rewire does not intentionally add account names or email addresses to AI requests, but user-provided text may contain identifying or sensitive information. Rewire does not use AI conversation content to train models and does not intentionally retain AI conversation logs server-side beyond the active request; downstream processing is governed by the applicable provider terms and its Business Associate Agreement.

HIPAA-aligned controls (US practitioners)

For practitioners operating in the US healthcare system, Rewire implements the following controls aligned with the HIPAA Security Rule:

- Unique user identification and strong authentication for all accounts
- Automatic session timeout after inactivity
- Role-based access controls preventing cross-practitioner data access
- Use of managed infrastructure that provides encryption at rest and HTTPS/TLS for data in transit
- End-to-end encryption of clinical free-text (client-side AES-256-GCM), so narrative content is unreadable by Rewire and its subprocessors
- PHI-access audit logging with a 6-year retention window

US-based healthcare providers requiring a Business Associate Agreement (BAA) may request one at privacy@rewire-emdr.com.

Data retention

- Active account data is retained for as long as the account remains active
- Practitioner account data is deleted within 30 days of account closure
- End user session data and journal entries are scheduled for deletion within 30 days of the end user's account closure; removal from a practitioner's roster does not itself delete the end user's account or history
- Billing records are retained for 7 years in accordance with applicable financial regulations
- Anonymised, aggregated analytics data (no personal identifiers) may be retained indefinitely for product improvement

04 — SUB-PROCESSORS

Third-party processors we use

rewire-emdr.com/privacy · Version 2.1 · Effective August 2, 2026 · Downloaded copy — current terms at rewire-emdr.com/privacy

PROCESSOR	PURPOSE	JURISDICTION	CERTIFICATION
Supabase	Database, authentication, file storage	US / EU (configurable)	SOC 2 Type II
AI provider (HIPAA-covered, under BAA)	Models used for AI session content generation	US (API processing)	Business Associate Agreement and provider terms apply
Cloudflare	Worker proxy for AI requests; DDoS and edge security	Global edge network	SOC 2 Type II, ISO 27001
Resend	Transactional and service email delivery	US	Provider terms and controls apply
Stripe	Payment processing	US / EU	PCI DSS Level 1
Contentsquare	Analytics on the public marketing website only; not loaded in the clinical application or authenticated portals	Global	Provider terms and controls apply

We review all sub-processor agreements for GDPR adequacy before engagement. Data transfers to the US are covered by Standard Contractual Clauses (SCCs) under GDPR Art. 46(2)(c). We will notify account holders of any material change to our sub-processor list at least 30 days in advance.

05 — AI-POWERED FEATURES

AI-Powered Features

Rewire uses third-party artificial intelligence service providers to power certain features, such as generating supportive responses, reflections, and summaries. When you use these features, the content you submit may be processed by these providers solely to deliver the feature to you. These providers act as our service providers under contract and are not permitted to use your content to train their models or for any purpose other than providing the service to us. Where this content includes health-related information, we are working to bring our AI processing under appropriate data protection terms, and we do not intentionally include your name or email in AI requests.

06 — YOUR RIGHTS (GDPR)

Data subject rights

Users in the EEA, UK, Switzerland, and equivalent jurisdictions have the following rights under GDPR (or applicable equivalent legislation):

- **Right of access (Art. 15):** Request a copy of all personal data we hold about you, including the source, purpose, and any third parties it has been shared with.
- **Right to rectification (Art. 16):** Request correction of inaccurate or incomplete personal data.
- **Right to erasure (Art. 17):** Request permanent deletion of your personal data. Note: billing records may be retained for the statutory minimum period.
- **Right to data portability (Art. 20):** Request your personal data in a structured, machine-readable format (JSON or CSV).
- **Right to restrict processing (Art. 18):** Request that we restrict processing in certain circumstances while a dispute is resolved.
- **Right to object (Art. 21):** Object to processing based on legitimate interests, including any direct marketing.

— **Right to withdraw consent:** Where processing is based on consent, withdraw it at any time without affecting the lawfulness of prior processing.

rewire-emdr.com/privacy · Version 2.1 · Effective August 2, 2026 · Downloaded copy — current terms at rewire-emdr.com/privacy

To exercise any of these rights: email privacy@rewire-emdr.com with the subject line "Data Subject Rights Request". We will respond within 30 days. You also have the right to lodge a complaint with your national supervisory authority (e.g. ICO in the UK, CNIL in France, or the relevant DPA in your country).

07 — SPECIAL CATEGORY DATA

Sensitive data and mental health information

Journal entries entered by users during sessions may constitute special category data under GDPR Art. 9, specifically data concerning health and mental wellbeing. We treat all journal entry data as special category data by default and apply the following additional protections:

- Journal entries and other clinical free-text are protected with client-side end-to-end encryption (AES-256-GCM with X25519 key wrapping): they are encrypted on the user device before storage, so neither Rewire nor its database provider can read them. Data is also transmitted over HTTPS/TLS and stored on infrastructure that provides encryption at rest.
- Journal entries are never shared with the assigning practitioner without explicit, in-app consent from the end user
- Journal entries are never used for AI model training, analytics, or any purpose other than direct service provision to the user
- Practitioners are contractually bound by our Terms of Service to obtain appropriate informed consent from clients before assigning Rewire, including consent to data collection and storage as described in this policy

08 — COOKIES & ANALYTICS

Cookies and tracking

The clinical application and authenticated portals use browser storage and session technologies needed for authentication and application functionality. They do not load advertising trackers, behavioural analytics, or device-fingerprinting technology.

The public marketing website uses Contentsquare to understand website usage and improve the site. This marketing-site analytics service may use cookies or similar technologies under Contentsquare's privacy controls. Rewire does not use marketing analytics data for clinical decision-making.

09 — CHANGES TO THIS POLICY

Policy updates

We will notify all active account holders by email of material changes to this policy at least 14 days before they take effect. The current version is always available at rewire-emdr.com/privacy. Continued use of the platform after the effective date of a revised policy constitutes acceptance of the updated terms.

For questions about this policy: privacy@rewire-emdr.com