HIPAA POLICY

HIPAA Compliance*at Rewire.*

Last updated: August 6, 2026 · Version 1.0 · Rewire App LLC

01 — OUR ROLE

How Rewire fits within HIPAA

Rewire App LLC is not a healthcare provider, health plan, or healthcare clearinghouse and does not represent itself as a HIPAA Covered Entity. When a therapist, group practice, treatment facility, or other Covered Entity uses Rewire to create, receive, maintain, or transmit protected health information on its behalf, Rewire acts as that organization's **Business Associate**.

In that role, Rewire applies the safeguards and contractual commitments described here and in its Business Associate Agreement. Covered Entities remain responsible for their own HIPAA obligations, clinical decisions, workforce practices, and appropriate use of the platform.

02 — ADMINISTRATIVE SAFEGUARDS

Governance, risk management, and workforce practices

Rewire maintains a written Security Risk Assessment and Security Policy addressing risks to the confidentiality, integrity, and availability of electronic protected health information. Rewire also maintains a workforce sanction policy and workforce security and privacy training requirements appropriate to each person's responsibilities.

These internal policy documents are maintained within Rewire's legal and compliance program and are **available to covered-entity partners on request**, subject to reasonable confidentiality and security controls.

03 — TECHNICAL SAFEGUARDS

Controls protecting electronic PHI

Rewire uses layered technical controls designed to limit access and protect information throughout its lifecycle:

- **End-to-end encryption:** journal entries and other clinical free-text are encrypted on the user device with AES-256-GCM. X25519 key wrapping supports authorized sharing, and Argon2id is used in password-based key protection. Rewire and its database provider cannot read the stored narrative content.
- **Encryption in transit:** application traffic is protected using HTTPS/TLS.
- **Unique user authentication:** each user accesses the platform through an individually assigned account or access credential.
- **Automatic session timeout:** authenticated sessions expire after inactivity to reduce the risk of unattended access.
- **Role-based access control:** permissions and database row-level controls restrict users to information associated with their role and authorized relationships.
- **Audit controls:** Rewire records PHI-access events and retains PHI-access audit logs for six years.

04 — BUSINESS ASSOCIATE AGREEMENTS

Contractual protection across the service chain

Rewire signs a Business Associate Agreement with covered-entity therapists and facilities when Rewire will handle PHI on their behalf. The current form and request process are available on our Business Associate Agreement page.

Rewire's upstream subprocessors that may participate in handling PHI are also covered by BAAs: **Anthropic** for AI processing, **Supabase** for database and authentication infrastructure, and **Cloudflare** for application hosting and edge services. Rewire limits disclosures to what is reasonably necessary to provide and secure the service.

05 — BREACH NOTIFICATION

Notice to covered-entity partners

If Rewire discovers a breach of unsecured PHI, Rewire will notify affected Covered Entities without unreasonable delay and no later than **10 business days after discovery**. Rewire will provide the information required for the Covered Entity's assessment and notifications to the extent that information is known and will supplement the notice as additional material facts become available.

06 — INCIDENT RESPONSE

Prepared response and recovery

Rewire maintains a written incident-response plan for identifying, containing, investigating, documenting, and recovering from security incidents. The plan establishes responsibilities, escalation paths, evidence-preservation expectations, and post-incident review procedures, including coordination with affected covered-entity partners where PHI may be involved.

07 — CONTACT

BAA requests and compliance questions

Covered entities may request a BAA, supporting compliance materials, or answers to HIPAA-related questions by emailing privacy@rewire-emdr.com.