

BUSINESS ASSOCIATE AGREEMENT

Your data, *protected by design.*

Last updated: August 2026 · Version 1.1 · Rewire App LLC

HOW TO READ THIS

This is the Business Associate Agreement (BAA) between Rewire App LLC and you — the licensed practitioner or facility (the "Covered Entity") who uses Rewire with the people you serve. By accepting it during onboarding, you and Rewire agree to the HIPAA obligations below. Rewire is engineered so that the sensitive things your clients write are **end-to-end encrypted and unreadable by Rewire**; this agreement covers the limited information Rewire does handle on your behalf.

Downloaded standard agreement copy — not a countersigned counterpart. Need a countersigned copy? Contact hello@rewire-emdr.com.

PREAMBLE

Parties & purpose

This Business Associate Agreement ("Agreement") is entered into between **Rewire App LLC**, 63 N Burritt Ave, Room 100 East PMB 1062, Buffalo, WY 82834 (the "Business Associate"), and the licensed mental-health provider, practice, or facility that accepts this Agreement during account onboarding (the "Covered Entity"). It takes effect on the date of that acceptance.

It governs any Protected Health Information ("PHI") that Rewire creates, receives, maintains, or transmits on the Covered Entity's behalf, and is designed so that Rewire's access to identifiable information is **minimized by design** (see Exhibit A). Capitalized terms not defined here carry the meanings given under the Health Insurance Portability and Accountability Act of 1996 and its regulations (45 C.F.R. Parts 160 and 164), as amended by the HITECH Act ("HIPAA").

SECTION 1

Permitted uses and disclosures

1.1 Service performance. Rewire may use or disclose PHI only as necessary to provide the Service to the Covered Entity, as permitted by this Agreement, or as Required by Law.

1.2 Minimum necessary. Rewire will request, use, and disclose only the minimum necessary PHI to accomplish the intended purpose, consistent with Exhibit A.

1.3 Management & administration. Rewire may use PHI for its proper management and administration or to carry out its legal responsibilities, provided any disclosures are Required by Law or made with reasonable assurances of confidentiality and breach notification.

1.4 De-identification / aggregation. Rewire may use PHI to create de-identified data (per 45 C.F.R. § 164.514(a)–(c)) and to provide data-aggregation services relating to the Covered Entity's health-care operations.

1.5 Prohibited uses. Rewire will **not** sell PHI, use PHI for marketing, or use PHI for its own independent purposes except as expressly permitted here.

SECTION 2

rewire-emdr.com/baa · Version 1.1 · Effective August 2026 · Downloaded copy — current terms at rewire-emdr.com/baa

Rewire's obligations

Rewire shall:

- Not use or disclose PHI other than as permitted by this Agreement or Required by Law.
- Use appropriate administrative, physical, and technical safeguards — including encryption of electronic PHI in transit and at rest — and comply with the HIPAA Security Rule (Subpart C of 45 C.F.R. Part 164).
- Report to the Covered Entity any use or disclosure not permitted by this Agreement, and any Breach of Unsecured PHI, promptly and no later than ten (10) business days after discovery, with the information required by 45 C.F.R. § 164.410 to the extent known to Rewire.
- Ensure that any subcontractor that handles PHI on Rewire's behalf agrees in writing to restrictions at least as protective as those here (see Exhibit B).
- Make PHI in a Designated Record Set available to the Covered Entity as needed to satisfy access (§ 164.524) and amendment (§ 164.526) obligations, subject to Section 2.1 below.
- Maintain and make available information needed for an accounting of disclosures (§ 164.528).
- To the extent Rewire carries out a Covered Entity obligation under the Privacy Rule, comply with the requirements that apply to that obligation.
- Make its internal practices, books, and records relating to PHI available to the Secretary of HHS for compliance determinations.
- Maintain reasonable access logs of personnel and systems accessing PHI.

2.1 No Designated Record Set maintained by Rewire

The Parties acknowledge and agree that Rewire does **not** maintain PHI in a Designated Record Set for or on behalf of the Covered Entity. The Covered Entity remains the custodian of the record of truth (for example, in its own clinical or EHR system) and will maintain a separate copy of all PHI it directs to Rewire, including all information needed to respond to individuals' access, amendment, and accounting requests. Where an individual directs such a request to Rewire, Rewire will refer the individual to the Covered Entity or, where Rewire knows the Covered Entity's identity, forward the request; the Covered Entity is solely responsible for granting or denying it.

2.2 Unsuccessful security incidents

The Parties acknowledge that unsuccessful security incidents — such as pings and other broadcast attacks on a firewall, denial-of-service attacks, port scans, and unsuccessful log-in attempts — occur in the normal course of business, and agree that this paragraph constitutes notice by Rewire to the Covered Entity of such unsuccessful security incidents. Rewire's reporting obligation above applies to Security Incidents and Breaches that are not unsuccessful security incidents.

SECTION 3

Covered Entity's obligations

3.1 The Covered Entity will notify Rewire of any limitation in its Notice of Privacy Practices, any change in or revocation of an individual's permission, and any restriction on use or disclosure it has agreed to, to the extent it affects Rewire's use or disclosure.

3.2 The Covered Entity will not request that Rewire use or disclose PHI in any manner that would not be permitted under HIPAA if done by the Covered Entity.

3.3 Identifier minimization (material term). The Covered Entity acknowledges the Service is designed for pseudonymous use and agrees to use, and to instruct the individuals it serves to use, **client codes or first names only** — and to not enter patient full names, addresses, or other direct identifiers into free-text fields where avoidable (see Exhibit A).

SECTION 4

Term and termination

rewire-emdr.com/baa · Version 1.1 · Effective August 2026 · Downloaded copy — current terms at rewire-emdr.com/baa

4.1 Term. This Agreement is effective on the acceptance date and continues until terminated or until all PHI is returned or destroyed.

4.2 Termination for cause. The Covered Entity may terminate upon Rewire's material breach not cured within thirty (30) days of notice.

4.3 Effect of termination. Upon termination, Rewire will return or destroy all PHI if feasible. Where infeasible, Rewire will extend the protections of this Agreement to such PHI and limit further uses or disclosures to those that make return or destruction infeasible.

SECTION 5

Miscellaneous

Regulatory references are to the section as in effect or amended. The Parties will amend this Agreement as necessary to comply with HIPAA, and ambiguities are resolved to permit compliance with HIPAA. There are no third-party beneficiaries. Section 4.3 survives termination. The Parties are independent contractors; nothing here creates a partnership, joint venture, or agency. This Agreement is governed by the law of the State of Wyoming, except where preempted by federal law.

EXHIBIT A

Data architecture & minimization

This Exhibit describes the limited information Rewire handles and how identifiability is minimized.

What Rewire is designed NOT to receive

Patient full legal names, dates of birth, addresses, Social Security numbers, medical record numbers from the Covered Entity's EHR, diagnoses entered as clinical codes, or insurance information.

What Rewire may receive or store on the Covered Entity's behalf

- A pseudonymous client code or first name chosen at the Covered Entity's direction;
- A login email address used solely for authentication and Service notifications (for code-based client accounts, not even this is stored);
- Self-directed session activity (session theme selected by the individual, completion status, self-reported distress ratings, mood);
- Free-text reflections and journal entries voluntarily written by the individual;
- Worksheet responses the individual voluntarily elects to share with the Covered Entity.

Safeguards

- **End-to-end encryption:** client reflections, journals, worksheet responses, and clinician notes are encrypted on the individual's device with keys derived from their own password. Rewire cannot read this content.
- Electronic PHI encrypted in transit (TLS) and at rest;
- Row-level access controls limiting each provider to their own clients' shared data;
- Reflections and worksheets default to private; sharing with the provider is opt-in by the individual;
- Access logging; no sale of data; no advertising use.

EXHIBIT B

Subcontractors

rewire-emdr.com/baa · Version 1.1 · Effective August 2026 · Downloaded copy — current terms at rewire-emdr.com/baa

Rewire uses the following subcontractors, each of which must be under a BAA or equivalent written assurance before PHI flows to them:

SUBCONTRACTOR	ROLE	STATUS
AI provider (HIPAA-covered)	AI feature (processes decrypted content the user chooses to send)	BAA in place
Supabase, Inc.	Database / auth hosting (stores encrypted content only)	BAA in place
Cloudflare, Inc.	Application hosting / CDN	BAA in place
Stripe, Inc.	Payments (no clinical PHI)	N/A

Questions or need a countersigned copy? Contact hello@rewire-emdr.com. This page reflects the current Business Associate Agreement offered to covered-entity practitioners and facilities; a signed counterpart is available on request.