Privacy Policy

Jounce Technologies, Inc.

Version 1.1 — Effective Date: May 5, 2026 | Last Updated: May 5, 2026

Jounce Technologies, Inc. (“Jounce,” “we,” “our,” or “us”) values your privacy and is committed to protecting the personal information you share with us. This Privacy Policy explains how we collect, use, share, and safeguard information when you use the Jounce website, mobile application, and related services (the “Platform”). By using the Platform, you consent to the data practices described in this Privacy Policy. If you do not agree, please discontinue use of the Platform.

Jounce's Platform is currently available to users in the United States only. This policy does not address data protection laws of other jurisdictions, including the European Union's General Data Protection Regulation (GDPR).

1. Information We Collect

1a. Information You Provide

- **Personal Information:** Name, address, phone number, email address, and payment details.
- **Account Information:** Username, password, and account preferences.
- **Child Information (provided by parent/legal guardian):** Child's first name, age or date of birth, and support needs relevant to matching with a suitable provider. This information is provided by and remains under the control of the parent or legal guardian. Clinical session notes, treatment plans, and similar records are maintained by the individual provider in their own systems and are not stored by Jounce.
- **Job Post Information:** When families submit Job Posts to find a Provider, we collect the content of the Job Post — typically including service category, scheduling preferences, location and availability, and a free-text description of the family's needs. Families should not include diagnoses, medical history, or other Protected Health Information in Job Post text fields. Sensitive health information is collected separately at the booking and intake stage, where HIPAA safeguards apply.
- **Health Information:** For families using Jounce's insurance billing integration (Phase II), formal diagnosis documentation and ICD-10 diagnostic codes provided by the family's healthcare provider, which are required by the insurance carrier for claims processing through Office Ally. Jounce operates as a HIPAA Business Associate for any Protected Health Information it receives in this capacity.
- **Provider Information:** Professional license numbers, certifications, credential documentation, service specialties, and availability.
- **Provider Application Information:** When Providers submit Applications in response to family Job Posts, we collect the content of the Application, including any message to the family, proposed availability, and indication of credentials and experience relevant to the request.

- **Provider Financial Information:** For all providers who accept payments through the Platform, tax identification numbers (SSN or EIN), banking information, and identity verification documents are collected and held by our payment partner Stripe, Inc., not by Jounce. See Section 3 for details.
- **Respite Care Provider Information:** For Respite Care, Home Health Aide (HHA), and Personal Care Aide (PCA) providers specifically, background check reports and supporting documentation, including criminal history search results, sex offender registry checks, applicable state child abuse and neglect registry checks, and identity verification records. Background checks are processed by our screening partner Checkr. See Section 5 for details.

1b. Information We Collect Automatically

- **Usage Data:** Device type, operating system, IP address, browser type, session duration, referring URLs, and feature interactions for analytics and Platform improvement.
- **Booking & Transaction Data:** Session dates, service types, payment amounts, and cancellation records.
- **Cookies and Tracking Technologies:** We use cookies, pixel tags, and similar technologies for essential site functionality (session management, authentication), analytics (Google Analytics or equivalent), and platform performance monitoring. See Section 10 for details on managing cookie preferences.

2. How We Use Your Information

We use collected information to:

- Match families with licensed providers based on support needs, location, language, and cultural preferences.
- Surface and curate Provider Applications in response to family Job Posts, and deliver matched Applications to the requesting family.
- Schedule, confirm, and manage appointments.
- Process payments, issue receipts, and provide HSA/FSA documentation through Stripe.
- Verify provider credentials and monitor ongoing license status.
- For Respite Care providers, conduct and periodically renew background checks through Checkr.
- Send session reminders, completion notifications, renewal reminders, and platform updates.
- Improve Platform functionality, matching quality, and user experience.
- Analyze aggregated usage patterns to improve service quality.
- Comply with legal, regulatory, FCRA, HIPAA, and COPPA obligations.
- Detect, prevent, and address fraud, security incidents, and Platform misuse.

3. Information Sharing

We do not sell your personal information. We may share information in the following limited circumstances:

3a. With Licensed Providers

Booking details and the child's support need information are shared with the matched provider at the time a session is booked, to enable the provider to deliver services. When a family submits a Job Post, the content of the Job Post (excluding the family's full identity, until selection) is shared with eligible Providers who may submit an Application. When a family selects a Provider in response to an Application, the family's contact and booking information is shared with the selected Provider only. Providers are bound by confidentiality obligations and, where applicable, HIPAA. Providers may only use this information to provide services to you and are contractually prohibited from using it for any other purpose. Clinical documentation generated during or after the session is maintained solely by the provider.

3b. With Payment Processor — Stripe

Jounce Technologies, Inc. is the merchant of record for all transactions on the Platform. Customers will see “JOUNCE” on their credit card or bank statements. All payments are processed through Stripe, Inc. (“Stripe”), a PCI-DSS Level 1 certified payment processor.

Specifically, Stripe handles:

- **Payment processing:** Family credit card and debit card information is transmitted directly to Stripe and is never stored on Jounce servers. Jounce receives only tokenized references.
- **Provider Connect accounts:** All providers who accept payments create Stripe Connect Express accounts. Stripe performs Know-Your-Customer (KYC) verification, collects provider tax identification numbers, bank account information, and identity documents, and holds funds on behalf of providers.
- **Funds management:** Provider funds are held by Stripe, not by Jounce. Jounce is not a money services business or money transmitter.
- **Tax reporting:** Stripe generates IRS Form 1099-K and 1099-NEC for eligible providers automatically.

Stripe's privacy practices are governed by its own privacy policy, available at stripe.com/privacy.

3c. With Background Screening Partner — Checkr

For Respite Care, HHA, and PCA providers only, background check data is processed through Checkr, Inc. (“Checkr”), our FCRA-compliant screening partner. Checkr collects provider identifying information (including Social Security Number and date of birth) directly and conducts:

- National criminal database search
- County-level criminal records searches
- Sex offender registry checks
- State-specific child abuse and neglect registry checks (where applicable)

- Identity verification
- Global watchlist screening

Providers must provide separate consent to Checkr as part of the background check process. Completed reports are shared with Jounce for adjudication. Checkr's privacy practices are governed by its own privacy policy, available at checkr.com/privacy.

See Section 5 below for your rights under the Fair Credit Reporting Act (FCRA) and applicable state laws.

3d. With Insurance Billing Partner — Office Ally (Phase II)

When Jounce enables insurance billing functionality (planned for Phase II), relevant session information, diagnostic codes, and formal diagnosis documentation will be shared with Office Ally, our HIPAA-compliant insurance clearinghouse, for claims processing. A formal diagnosis is required by the insurance carrier before any insurance claim can be submitted. Office Ally is a HIPAA Business Associate and processes data under a Business Associate Agreement (BAA) with Jounce.

3e. With Analytics & Operations Tools

We use third-party tools for platform analytics, communications, and operations. At launch, this includes:

- Google Analytics (or equivalent) for usage analytics. IP addresses are anonymized where possible.
- Email service providers for transactional emails (session confirmations, receipts, renewal reminders).
- Customer support tools for responding to user inquiries.

All such tools are vetted for security compliance and data minimization practices. A current list of third-party service providers is available upon request at privacy@jouncein.com.

3f. With Legal Authorities

We may disclose information when required by law, subpoena, or court order; to enforce our Terms of Service; or to protect the rights, property, or safety of Jounce, our users, or the public.

3g. Business Transfers

If Jounce is involved in a merger, acquisition, financing, reorganization, or sale of assets, personal information may be transferred as part of the transaction, subject to the commitments in this Privacy Policy. Users will be notified of material changes resulting from any such transaction.

We will update this section as new third-party integrations are added. Users will be notified of any material changes.

4. HIPAA & Protected Health Information

Where Jounce facilitates the provision of covered health services, we operate as a HIPAA Business Associate to the licensed providers on our Platform. Health information collected through the Platform is handled in accordance with:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The HIPAA Privacy Rule (45 CFR §§ 164.500–164.534)
- The HIPAA Security Rule (45 CFR §§ 164.302–164.318), including required administrative, physical, and technical safeguards
- The HIPAA Breach Notification Rule (45 CFR §§ 164.400–164.414)

We maintain Business Associate Agreements (BAAs) with all covered third parties that process Protected Health Information (PHI) on our behalf, including Office Ally (Phase II) and any other future partners. We do not use PHI for marketing purposes.

For HIPAA-related requests or to exercise rights regarding Protected Health Information specifically, please email us at privacy@jouncein.com with “HIPAA Request” in the subject line.

5. Background Checks & FCRA Rights (Respite Care Providers)

For Respite Care, HHA, and PCA providers only, Jounce conducts background checks through Checkr prior to Platform activation and annually thereafter.

5a. Your FCRA Rights

Background checks are “consumer reports” subject to the Fair Credit Reporting Act (FCRA, 15 U.S.C. § 1681 et seq.) and applicable state consumer reporting laws. As a provider undergoing a background check, you have the following rights:

- **Right to consent:** You must provide separate written consent before a background check is initiated.
- **Right to a copy:** You may request a free copy of your background check report from Checkr.
- **Right to dispute:** You may dispute the accuracy or completeness of any information in your report directly with Checkr.
- **Right to pre-adverse action notice:** If Jounce intends to reject or remove you based in whole or in part on a background check, you will receive a pre-adverse action notice, a copy of the report, and a summary of your FCRA rights. You will have at least five (5) business days to respond before a final decision is made.
- **Right to adverse action notice:** If an adverse decision is made, you will receive a final adverse action notice, including the name, address, and telephone number of Checkr and your right to request further information.

5b. Annual Renewal

Background checks expire 365 days after the date of clearance. Jounce will notify providers at 60, 30, and 14 days before expiration, and will initiate renewal automatically if not started by the provider. Providers cannot accept new bookings while their background check is expired.

5c. State-Specific Requirements

Providers may be subject to state-specific child abuse and neglect registry checks and other state licensing requirements, depending on the state in which they practice. Applicable state checks are included in every respite provider's background check package. As Jounce expands into additional states, we will update our screening packages to include any state-specific checks required by local law.

6. Provider Credential & License Verification

Jounce verifies the professional credentials, licenses, and certifications of every provider on the Platform before activation, and monitors license status on an ongoing basis. This applies to all provider categories, including licensed therapists (ABA, speech-language, occupational, behavioral, art, music, child life specialists), educational support providers, and respite care providers.

6a. Verification Sources

Credential verification may include:

- Direct verification with state licensing boards (e.g., state boards of psychology, behavior analysis, speech-language pathology, occupational therapy, nursing).
- Verification with national certification bodies (e.g., Behavior Analyst Certification Board, American Speech-Language-Hearing Association).
- Review of original credential documentation submitted by the provider.
- Ongoing monitoring of license status, expiration dates, and any disciplinary actions reported by the issuing authority.

6b. Provider Consent

By creating a provider account on the Platform, providers consent to Jounce conducting credential verification and ongoing license monitoring, including retrieval of publicly available licensure and disciplinary information from applicable state and national regulatory bodies. Credentialing information collected for verification purposes is stored securely and used only to maintain the integrity of the Platform.

6c. Consequences of License Issues

If a provider's license expires, is suspended, or is revoked, Jounce will promptly suspend the provider's ability to accept new bookings and notify the provider of the issue. Providers may appeal or respond to verification findings by contacting support@jouncein.com.

7. Children's Privacy & COPPA Compliance

Jounce's Platform is designed exclusively for use by parents and legal guardians on behalf of their children. We do not knowingly permit children under the age of 18 to create accounts, and we do not collect personal information directly from children of any age.

All child-related information — including name, age, support needs — is submitted exclusively by the child's parent or legal guardian, who retains full control over that information.

7a. COPPA Parental Rights

In compliance with the Children's Online Privacy Protection Act (COPPA, 15 U.S.C. §§ 6501–6506), parents and legal guardians have the right to:

- Review any personal information collected about their child.
- Request correction or deletion of their child's information at any time.
- Withdraw consent for collection of their child's data, subject to any legal retention obligations.
- Refuse further collection or use of their child's information.

To exercise any of these rights, please contact us at privacy@jouncein.com. We will respond within 30 days.

7b. COPPA & HIPAA Interaction

Where a child's therapy records constitute Protected Health Information (PHI), both COPPA and HIPAA may apply simultaneously. In all cases, the parent or legal guardian controls access to and decisions regarding the child's information, consistent with both regimes.

8. Data Protection & Security

We implement administrative, physical, and technical safeguards as required by the HIPAA Security Rule (45 CFR §§ 164.308–164.316). These include:

- HIPAA-compliant data handling and storage.
- Encryption of all data in transit using industry-standard TLS protocols.
- Encryption of data at rest on secure, access-restricted servers.
- Role-based access controls — only authorized personnel can access sensitive data, and access is logged.
- Routine security audits and vulnerability assessments.
- Business Associate Agreements (BAAs) with all third parties that handle Protected Health Information.
- Incident response procedures in accordance with the HIPAA Breach Notification Rule and applicable state data breach notification laws.

8a. International Data Transfers

Some of our service providers (including Stripe, Checkr, and analytics tools) may process or store data on servers located outside your specific state, but within the United States. Jounce does not currently transfer user data outside the United States.

8b. Data Breach Notification

In the event of a data breach that compromises your personal information, we will notify affected users in accordance with applicable federal and state laws, including the HIPAA Breach Notification Rule and applicable state data breach notification statutes. Notifications will be made without unreasonable delay, generally within 60 days of discovery for breaches involving PHI.

9. Data Retention

We retain personal information for as long as necessary to fulfill the purposes for which it was collected, comply with legal obligations, resolve disputes, and enforce agreements. Standard retention periods include:

- **Account & Profile Information:** Retained for the duration of the account, plus 3 years after account closure.
- **Booking and Session Records:** Booking history, session metadata (date, time, service type, provider, family), and payment records are retained for a minimum of 6 years to meet applicable HIPAA recordkeeping requirements for Business Associates. Jounce does not store clinical session notes or treatment records; those are maintained by the individual provider in their own systems.
- **Job Post and Application Records:** Job Posts and Applications are retained for the duration of the active matching window plus 2 years for fraud prevention, dispute resolution, and platform integrity.
- **Payment Records:** Retained for 7 years in accordance with IRS and financial recordkeeping requirements.
- **Background Check Records (Respite Care providers):** Cleared reports retained for the duration of the provider's active status plus 3 years after account closure. Rejected reports retained only as long as necessary to complete the FCRA adverse action process, typically 90 days post-notice.
- **Usage & Analytics Data:** Retained for up to 2 years in aggregated or de-identified form.

Following the applicable retention period, data is securely deleted or anonymized. You may request early deletion of your personal information (excluding data subject to legal retention obligations) by contacting privacy@jouncein.com.

10. Your Rights

All users have the right to:

- **Access:** Request a copy of the personal information we hold about you.
- **Correction:** Request correction of inaccurate or incomplete information.
- **Deletion:** Request deletion of your personal information, subject to legal retention requirements.
- **Withdrawal of Consent:** Withdraw consent for non-essential data processing at any time.

- **Data Portability:** Request a structured, machine-readable copy of your data where technically feasible.
- **Communication Preferences:** Opt out of marketing communications at any time by clicking the unsubscribe link in our emails or updating your account preferences. You cannot opt out of transactional communications (e.g., booking confirmations, renewal notices) while your account is active.

To exercise any of these rights, contact us at privacy@jouncein.com. We will respond within 30 days.

11. Cookies & Tracking Technologies

Jounce uses cookies and similar technologies to provide, improve, and analyze the Platform. Types of cookies we use:

- **Essential cookies:** Required for core functionality, including authentication and session management. These cannot be disabled without affecting Platform usability.
- **Analytics cookies:** Collect aggregated usage data to help us understand how users interact with the Platform (e.g., Google Analytics). These are optional.
- **Functional cookies:** Remember your preferences (e.g., language, saved searches) to personalize your experience.

You can manage or disable cookies through your browser settings. Disabling essential cookies may prevent parts of the Platform from functioning correctly.

11a. Do Not Track Signals

Jounce does not currently respond to “Do Not Track” (DNT) signals transmitted by web browsers, as there is no industry consensus on how such signals should be interpreted. You may manage tracking through browser cookie settings and by opting out of analytics tools directly (e.g., Google's opt-out browser add-on).

12. California Residents — CCPA/CPRA Rights

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA):

- **Right to Know:** You may request disclosure of the categories and specific pieces of personal information we have collected about you in the past 12 months, the sources of that information, the purposes for collecting it, and the categories of third parties with whom it has been shared.
- **Right to Delete:** You may request deletion of your personal information, subject to certain exceptions (e.g., legal obligations, fraud prevention, completion of a transaction).
- **Right to Correct:** You may request correction of inaccurate personal information.
- **Right to Opt-Out of Sale or Sharing:** Jounce does not sell or share personal information for cross-context behavioral advertising. If this practice changes, we will provide a prominent opt-out mechanism before doing so.

- **Right to Limit Use of Sensitive Personal Information:** You may limit our use of sensitive personal information (such as health data and precise geolocation) to purposes necessary for providing services.
- **Right to Non-Discrimination:** You will not be discriminated against for exercising your CCPA/CPRA rights.

To exercise California rights, contact us at privacy@jouncein.com with the subject line "California Privacy Request." We will verify your identity and respond within 45 days, with a possible 45-day extension if needed.

13. New York & New Jersey Residents

Jounce currently operates primarily in New York and New Jersey during its soft launch phase. As we expand into additional states, we will update this section to reflect applicable state-specific protections. Current state-specific protections include:

13a. New York SHIELD Act

Jounce implements reasonable administrative, technical, and physical safeguards for private information in accordance with the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act. In the event of a data breach affecting New York residents, we will notify affected individuals and the New York Attorney General as required.

13b. New Jersey Data Breach Notification

In the event of a data breach affecting New Jersey residents, we will notify affected individuals and the New Jersey Division of State Police, Cyber Crimes Unit, as required by the New Jersey data breach notification statute (N.J.S.A. 56:8-161 et seq.).

14. Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or Platform features. Material changes will be communicated via email or in-app notification at least 14 days before they take effect. Your continued use of the Platform after the effective date constitutes acceptance of the updated Policy. The "Last Updated" date at the top of this policy indicates when the most recent changes were made.

15. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or your personal data, please contact us:

- **Email:** privacy@jouncein.com
- **Website:** jouncein.com

For HIPAA-related requests, please include "HIPAA Request" in the subject line.

For California Privacy Rights requests, please include “California Privacy Request” in the subject line.

For FCRA / background check requests (Respite Care providers), please include “FCRA Request” in the subject line, or contact Checkr directly at checkr.com.

privacy@jouncein.com · jouncein.com