

RCMS Privacy Policy

Effective Date	Last Reviewed	Version
01/01/2026	05/10/2026	2.0

WHO WE ARE

Recovery Outcomes Institute, Inc ("ROI," "we," "us," or "our") is a Florida-based organization dedicated to advancing recovery capital research, assessment, and support services. We operate the Recovery Capital Management System ("RCMS" or the "Platform"), a software-as-a-service platform designed to help treatment courts, recovery residences, peer support organizations, healthcare providers, and other authorized entities assess, track, and support individuals in recovery.

This Privacy Policy describes how we collect, use, share, and protect personal information through RCMS, our website, and any other locations where this policy is linked or posted. This policy also explains your rights and choices regarding your personal information and how to contact us with questions.

We understand the sensitive nature of recovery-related information and are committed to protecting the privacy and confidentiality of all individuals whose information we process.

TABLE OF CONTENTS

- Information We Collect
- How We Use Information
- How We Share Information
- Data Security and Protection
- Data Retention and Deletion
- Your Rights and Choices
- HIPAA Compliance
- 42 CFR Part 2 Compliance
- State-Specific Privacy Rights
- Adults Only Service
- International Data Transfers
- Self-Directed Access (Future)
- Third-Party Services
- Changes to This Policy
- Contact Information

INFORMATION WE COLLECT

We collect information in several ways depending on how you interact with RCMS and the capacity in which you use our Platform:

Information Provided Directly

- **Account Information:** Name, email address, phone number, professional role, and organizational affiliation when you register for an account.
- **Participant Information:** For clients and participants enrolled by a Customer organization, this may include name, date of birth, contact information, case identifiers, and demographic information as entered by authorized organizational staff.
- **Assessment Data:** Recovery capital assessment responses, including information about personal, social, community, and cultural recovery capital domains.
- **Progress and Outcome Data:** Goals, milestones, program participation records, and outcome tracking information.
- **Communications:** Information you provide when contacting us for support, feedback, or inquiries.

Information Collected Automatically

- **Usage Data:** Information about how you interact with RCMS, including features accessed, pages viewed, and actions taken.
- **Device and Browser Information:** IP address, browser type, operating system, device identifiers, and other technical information.
- **Cookies and Similar Technologies:** We use cookies and similar tracking technologies to maintain session information, remember preferences, and analyze Platform usage.

Sensitive Personal Information

Given the nature of RCMS, we may process sensitive personal information including health-related information, substance use history, mental health information, and court involvement data. This information is collected and processed only as necessary to provide recovery support services, conduct assessments, and fulfill our contractual obligations to Customer organizations. We implement enhanced safeguards for all sensitive personal information.

HOW WE USE INFORMATION

We use the information we collect for the following purposes:

- **Service Delivery:** To provide, maintain, and improve RCMS, including conducting recovery capital assessments, tracking participant progress, and generating reports for authorized users.
- **Account Administration:** To create and manage user accounts, authenticate users, and provide account-related communications.
- **Customer Operations:** To support our Customer organizations' case management, participant monitoring, and compliance reporting as directed by authorized organizational personnel.
- **Research and Analytics:** To conduct de-identified, aggregate research on recovery outcomes, validate assessment tools, and improve recovery support practices, in accordance with the RCMS Research Consent and applicable Business Associate Agreements. Individual-level research participation requires separate informed consent.
- **Communication:** To respond to inquiries, provide customer support, send service-related notices, and communicate about Platform updates.

- **Security and Compliance:** To detect, prevent, and address technical issues, security threats, fraud, and violations of our Terms of Use.
- **Legal Compliance:** To comply with applicable laws, regulations, legal processes, and governmental requests.

HOW WE SHARE INFORMATION

We do not sell personal information. We do not use identifiable personal information for advertising, marketing, or commercial profiling. We share information only in the following circumstances:

With Customer Organizations

Participant information is shared with the Customer organization that enrolled the participant (such as a treatment court, recovery residence, peer support organization, or healthcare provider) and authorized staff members within that organization. Access is limited based on role-based permissions established by your organization's administrator. Where the Customer organization is a HIPAA Covered Entity, this sharing occurs under an executed Business Associate Agreement.

Service Providers (Subprocessors)

We engage third-party service providers to perform functions on our behalf. These providers are contractually obligated to protect personal information and may only use it to provide services to us. The categories of subprocessors we engage include:

- Cloud infrastructure and application hosting
- Database and data storage services
- Transactional email delivery services
- Customer relationship management and support tools
- Communication and meeting tools
- Productivity and business operations tools

A current list of specific subprocessors is available to Customer organizations on request. Where a subprocessor handles Protected Health Information, ROI executes a Business Associate Agreement with that subprocessor consistent with the obligations ROI owes to Covered Entities.

Research Partners

With appropriate consent and data use agreements, we may share de-identified or limited data sets with academic research partners for recovery capital research. Identifiable information is shared only with explicit participant consent and IRB approval where required.

Legal Requirements

We may disclose information when required by law, subpoena, court order, or government request, or when we believe disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request. Where information is subject to 42 CFR Part 2, we apply the heightened restrictions of Part 2 to any disclosure in response to legal process, in accordance with 42 CFR §§ 2.61–2.67.

Business Transfers

If we are involved in a merger, acquisition, or sale of assets, personal information may be transferred as part of that transaction. We will provide notice before personal information becomes subject to a different privacy policy.

DATA SECURITY AND PROTECTION

We implement comprehensive technical, administrative, and physical safeguards designed to protect personal information from unauthorized access, use, alteration, and disclosure. Our security measures include:

- **Encryption:** All data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 encryption.
- **Access Controls:** Role-based access controls ensure users can only access information necessary for their authorized functions.
- **Authentication:** Strong password requirements and optional multi-factor authentication protect user accounts.
- **Audit Logging:** Comprehensive logging tracks access to sensitive information for security monitoring and compliance purposes.
- **Security Assessments:** Regular security assessments, vulnerability scans, and penetration testing identify and address potential vulnerabilities.
- **Personnel Training:** All ROI personnel receive privacy and security training, and access to personal information is limited to those with a business need.

While we strive to protect personal information, no method of transmission over the internet or electronic storage is completely secure. We cannot guarantee absolute security, but we commit to promptly investigating and responding to any suspected security incidents in accordance with our Incident Response Policy and applicable Business Associate Agreements.

DATA RETENTION AND DELETION

We retain personal information for as long as necessary to fulfill the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law. Retention periods are determined based on:

- The duration of our relationship with you and your Customer organization
- Contractual obligations with Customer organizations, including Business Associate Agreements
- Legal retention requirements under HIPAA, 42 CFR Part 2, applicable state laws, and applicable records retention rules
- Statute of limitations for potential legal claims
- Research purposes with appropriate consent

Customer organizations may have specific retention requirements that exceed our standard retention periods. When personal information is no longer needed, it is securely deleted or de-identified in accordance with applicable regulations.

Deletion of personal information is governed by the RCMS Data Deletion Policy. Deletion requests are routed and executed in accordance with that policy, the executed Business Associate Agreement (where applicable), and the rights described in the "Your Rights and Choices" section below.

YOUR RIGHTS AND CHOICES

Depending on your jurisdiction and the nature of your relationship with ROI, you may have certain rights regarding your personal information. The mechanism for exercising these rights depends on whether ROI holds your information as a Business Associate of a Covered Entity, as a service provider to a non-HIPAA Customer organization, or as a controller under applicable state privacy law.

Rights Under HIPAA

Where ROI holds your Protected Health Information on behalf of a HIPAA Covered Entity, your rights of access, amendment, accounting of disclosures, and restriction under HIPAA (45 C.F.R. §§ 164.524, 164.526, 164.528, and 164.522) are exercised through that Covered Entity. The Covered Entity is responsible for receiving, evaluating, and fulfilling such requests, and ROI assists the Covered Entity as required by the executed Business Associate Agreement.

To exercise rights under HIPAA, please contact the Customer organization that enrolled you in the program (such as your treatment court coordinator, recovery residence administrator, or healthcare provider). They will work with us to fulfill your request in accordance with applicable law and procedures.

Rights Under State Privacy Laws

Residents of states with comprehensive privacy laws — including California (CCPA/CPRA), Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), and other states with similar laws — may have direct rights to access, correct, delete, obtain a portable copy of, or opt out of certain processing of their personal information.

ROI honors direct deletion requests and other applicable rights requests from state residents under their respective state privacy laws where ROI acts as a controller and not solely as a processor on behalf of a Covered Entity. Where ROI acts solely as a processor or Business Associate, requests are routed to the Customer organization (controller or Covered Entity) responsible for the information.

To submit a direct rights request to ROI under applicable state law, please contact us using the information below. We will verify your identity before fulfilling any request and will respond within the timeframes required by applicable law. We do not discriminate against individuals for exercising privacy rights.

Rights Under 42 CFR Part 2

Where your information is held under a Customer organization that is a Part 2 program, additional protections apply under 42 CFR Part 2. Requests to access, amend, or limit disclosure of Part 2 records are exercised through the Part 2 program in accordance with Part 2 procedures and applicable consents.

General Rights and Choices

Regardless of the legal regime that applies to your information, you may always:

- Contact ROI with questions about how your information is handled.
- Withdraw consent for inclusion of your de-identified data in future research, in accordance with the RCMS Research Consent.

- Submit a complaint to the appropriate regulatory authority, including the U.S. Department of Health and Human Services Office for Civil Rights for HIPAA matters or your state attorney general for state privacy law matters.

HIPAA COMPLIANCE

When RCMS is used by HIPAA Covered Entities (healthcare providers, health plans, or healthcare clearinghouses) or their Business Associates, we may receive, create, maintain, or transmit Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act ("HIPAA").

In these circumstances, we enter into Business Associate Agreements with Covered Entities (or with upstream Business Associates) that govern our use and disclosure of PHI. Our obligations with respect to PHI are set forth in those agreements and may provide additional protections beyond this Privacy Policy.

Not all Customer organizations using RCMS are HIPAA Covered Entities. Recovery residences, peer support organizations, treatment courts, and certain other entities may use RCMS without being subject to HIPAA. In those cases, ROI handles information in accordance with this Privacy Policy, the Customer organization's instructions, and applicable state privacy and confidentiality laws.

If you have questions about how your PHI is handled, please contact the Customer organization that enrolled you in the program, as they are responsible for fulfilling individual rights requests under HIPAA.

42 CFR PART 2 COMPLIANCE

Where a Customer organization is a federally-assisted substance use disorder treatment program subject to 42 CFR Part 2 ("Part 2"), records created, received, maintained, or transmitted by RCMS on behalf of that organization are subject to the heightened confidentiality requirements of Part 2 in addition to HIPAA.

ROI handles such records in accordance with the executed Business Associate Agreement, including the Part 2 provisions of that agreement, and applicable Part 2 regulations. This includes restrictions on use and disclosure under 42 CFR § 2.12, the redisclosure prohibition notice required by § 2.32, the legal process restrictions of §§ 2.61–2.67, and the requirement that any subprocessor handling Part 2 records be bound by equivalent obligations.

Customer organizations are responsible for obtaining patient consents that comply with 42 CFR § 2.31 prior to entering Part 2 records into RCMS, and for notifying ROI of any restrictions on use or disclosure that result from such consents or applicable law.

STATE-SPECIFIC PRIVACY RIGHTS

California Residents

California residents have rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), including the right to know what personal information we collect, the right to delete personal information, the right to correct inaccurate personal information, the right to opt out of the sale or sharing of personal information (we do not sell or share personal information for cross-context behavioral advertising), the right to limit use of sensitive personal information, and the right to non-discrimination for exercising privacy rights.

Other State Privacy Laws

Residents of Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), and other states with comprehensive privacy laws have similar rights under their respective state laws. We honor these rights for all eligible residents, subject to applicable exemptions and the framework described under "Your Rights and Choices" above.

ADULTS ONLY SERVICE

RCMS is intended for use by and about adults aged 18 and older. ROI does not knowingly collect or process personal information about individuals under the age of 18.

Customer organizations are responsible for confirming the adult status of participants whose information they enter into RCMS, and for ensuring that RCMS is not used to collect, store, or process information about individuals under 18. Customer organizations agree to this responsibility through their executed Master Service Agreement and Business Associate Agreement with ROI.

If we become aware that information about an individual under 18 has been entered into RCMS, we will work with the relevant Customer organization to remove the information promptly.

INTERNATIONAL DATA TRANSFERS

RCMS is operated from the United States. If you access RCMS from outside the United States, please be aware that your information may be transferred to, stored, and processed in the United States where our servers are located. By using RCMS, you consent to the transfer of your information to the United States, which may have different data protection laws than your country of residence.

SELF-DIRECTED ACCESS (FUTURE)

ROI does not currently support direct individual signup for RCMS. Upon launch of self-directed access, this Privacy Policy will be updated to describe how individuals using RCMS without an organizational affiliation may submit rights requests directly to ROI, including the verification process and timelines that will apply. The Terms of Use and Data Deletion Policy will be updated in parallel.

THIRD-PARTY SERVICES

RCMS may contain links to third-party websites or services. This Privacy Policy does not apply to those third-party services. We encourage you to review the privacy policies of any third-party services you access through RCMS.

CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices or applicable law. We will notify you of material changes by posting the updated Privacy Policy on our website with a new effective date. If we make significant changes that affect your rights, we will provide additional notice, such as email notification or an in-app announcement. Your continued use of RCMS after the effective date constitutes acceptance of the updated Privacy Policy.

CONTACT INFORMATION

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us:

Recovery Outcomes Institute

Email: info@recoveryoutcomes.org

Website: www.recoveryoutcomes.org

For Customer organization participants with questions about how your information is used, please contact your Customer organization's administrator (such as your treatment court coordinator, recovery residence administrator, healthcare provider, or peer support program contact), who can work with us to address your concerns.