

R2AI, LLC (known as RAICO)

Privacy Policy

Effective Date: April 13, 2026

<https://raicoapp.com>

Table of Contents

- Introduction
- Data Protection Officer
- How We Collect and Use Your Personal Information
- Use of the RAICO Website
- Cookies and Tracking Technologies
- Use of RAICO Services
- Sharing Information with Third Parties
- Transferring Personal Data to the U.S.
- Data Subject Rights
- Security of Your Information
- Data Storage and Retention
- Children's Data
- HIPAA and Protected Health Information
- Questions, Concerns, or Complaints

Introduction

RAICO is a healthcare artificial intelligence company specializing in prior authorization automation and clinical document processing workflows. Our platform leverages advanced AI and machine learning to streamline healthcare administrative processes, reduce provider burden, and accelerate patient access to care.

We understand that you are aware of and care about your own personal privacy interests, and we take that seriously. This Privacy Policy describes RAICO's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognize that information privacy is an ongoing responsibility, and so we will from time to time update this Privacy Policy as we undertake new personal data practices or adopt new privacy policies.

Given the nature of our work in healthcare, we are especially committed to maintaining the highest standards of data protection. Our privacy practices are designed to align with HIPAA, SOC 2 Type II, and other applicable data protection regulations.

Data Protection Officer

RAICO is headquartered in the United States. RAICO has appointed an internal data protection officer for you to contact if you have any questions or concerns about RAICO's personal data policies or practices. If you would like to exercise your privacy rights, please direct your query to a RAICO administrator.

How We Collect and Use Your Personal Information

RAICO collects personal information about its website visitors, customers, and the healthcare organizations that use our platform. This information is generally limited to:

- Name and job title
- Employer or healthcare organization name
- Work address, email, and phone number
- Account credentials and authentication data
- Usage data and interaction logs within the RAICO platform
- Technical information such as IP address, browser type, and device identifiers

We use this information to provide our services, improve our platform, communicate with customers, and fulfill our contractual obligations.

We do not sell personal information to anyone and only share it with third parties who are facilitating the delivery of our services, as described further in this policy.

From time to time, RAICO may receive personal information about individuals from third parties, such as healthcare organizations that integrate with our platform or referral partners. This information is used solely to facilitate the delivery of our services.

Use of the RAICO Website

As is true of most websites, raicoapp.com collects certain information automatically and stores it in log files. This information may include internet protocol (IP) addresses, the region or general location where your computer or device is accessing the internet, browser type, operating system, and other usage information about the use of the RAICO website, including a history of the pages you view.

We use this information to help us design our site to better suit our users' needs, diagnose problems with our server, administer our website, analyze trends, track visitor movements, and gather broad demographic information that assists us in identifying visitor preferences.

RAICO has a legitimate interest in understanding how customers and potential customers use its website. This assists RAICO with providing more relevant products and services, and with providing appropriate staffing to meet customer needs.

Cookies and Tracking Technologies

RAICO uses cookies and similar tracking technologies on raicoapp.com to enhance your browsing experience, analyze website traffic, and understand user behavior. Cookies are small text files placed on your device that allow us to recognize your browser and capture certain information.

We use the following types of cookies:

- **Essential Cookies:** Required for the website to function properly, including session management and security features.
- **Analytics Cookies:** Help us understand how visitors interact with our website by collecting and reporting information anonymously.
- **Functional Cookies:** Enable enhanced functionality and personalization, such as remembering your preferences.

You can control cookies through your browser settings. Please note that disabling certain cookies may affect the functionality of our website.

Use of RAICO Services

When you use RAICO's prior authorization and document processing services, we may process data on behalf of your healthcare organization. In this capacity, RAICO acts as a data processor (or business associate under HIPAA), and the healthcare organization remains the data controller (or covered entity).

The types of data processed through our services may include clinical documents, prior authorization requests, insurance information, and related healthcare administrative data. This data is processed solely for the purposes of providing our contracted services and is handled in accordance with our Business Associate Agreements (BAAs) and applicable privacy regulations.

RAICO does not use Protected Health Information (PHI) processed through our services for marketing, advertising, or any purpose unrelated to the delivery of contracted services.

Sharing Information with Third Parties

The personal information RAICO collects from you is stored in one or more databases hosted by third-party cloud service providers located in the United States. These third parties do not use or have access to your personal information for any purpose other than cloud storage, retrieval, and the delivery of infrastructure services.

We do not reveal your personal data to non-RAICO persons or businesses for their independent use unless:

- You request or authorize it;
- The information is provided to comply with the law (for example, in response to a search warrant, subpoena, or court order);
- It is necessary to enforce an agreement we have with you, or to protect our rights, property or safety, or the rights, property or safety of our employees or others;
- The information is provided to our agents, vendors, or service providers who perform functions on our behalf under appropriate data protection agreements;
- It is necessary to address emergencies or acts of God; or
- It is necessary to address disputes, claims, or to persons demonstrating legal authority to act on your behalf.

We may disclose aggregated, de-identified information that cannot reasonably be used to identify you to our partners, service providers, or other third parties for analytics, research, or promotional purposes.

Transferring Personal Data to the U.S.

RAICO has its headquarters in the United States. Information we collect about you will be processed in the United States. By using RAICO's services, you acknowledge that your personal information will be processed in the United States.

For users located in the European Economic Area (EEA) or the United Kingdom, the United States has not received a finding of "adequacy" from the European Union under Article 45 of the GDPR. Pursuant to Article 46 of the GDPR, RAICO provides for appropriate safeguards by entering binding, standard data protection clauses, enforceable by data subjects in the EEA and the UK.

RAICO endeavors to apply suitable safeguards to protect the privacy and security of your personal data and to use it only consistent with your relationship with RAICO and the practices described in this Privacy Policy. RAICO also enters into data processing agreements and model clauses with its vendors whenever feasible and appropriate.

Data Subject Rights

The European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other applicable privacy laws provide certain rights for data subjects. These rights may include:

- Right to be informed about how your data is collected and used
- Right of access to your personal data
- Right to rectification of inaccurate data
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right of data portability
- Right to object to processing
- Rights related to automated decision making, including profiling

If you wish to confirm that RAICO is processing your personal data, or to have access to the personal data RAICO may have about you, please contact us at privacy@raicoapp.com.

You may also request information about the purpose of the processing, the categories of personal data concerned, who else may have received the data, what the source of the information was, and how long it will be stored. You have a right to correct the record of your personal data maintained by RAICO if it is inaccurate. You may request that RAICO erase that data or cease processing it, subject to certain exceptions.

Reasonable access to your personal data will be provided at no cost. If access cannot be provided within a reasonable time frame, RAICO will provide you with a date when the information will be provided. If for some reason access is denied, RAICO will provide an explanation as to why access has been denied.

Security of Your Information

RAICO takes the security of your personal information seriously. We implement administrative, technical, and physical safeguards designed to protect your data against unauthorized access, alteration, disclosure, or destruction. Our security measures include:

- Encryption of data in transit (TLS/HTTPS) and at rest
- Role-based access controls and least-privilege principles
- Regular security assessments and vulnerability scanning
- Comprehensive audit logging and monitoring
- Network segmentation and firewall protections

RAICO is actively pursuing SOC 2 Type II certification and maintains security practices aligned with industry-recognized frameworks. Our infrastructure is hosted on Microsoft Azure with enterprise-grade security controls.

Data Storage and Retention

Your personal data is stored by RAICO on servers and cloud-based database management services located in the United States. RAICO retains service data for the duration of the customer's business relationship with RAICO and for a period of time thereafter as necessary for legitimate business purposes, legal compliance, dispute resolution, and enforcement of our agreements.

All personal data that RAICO controls may be deleted upon verified request from data subjects or their authorized agents, subject to applicable legal retention requirements. For more information on where and how long your personal data is stored, and for more information on your rights of erasure and portability, please contact a RAICO administrator.

Children's Data

RAICO's services are designed for use by healthcare organizations and their authorized personnel. We do not knowingly collect personal information directly from children under the age of 13. If we become aware that we have inadvertently collected personal information from a child under 13, we will take steps to delete such information promptly.

HIPAA and Protected Health Information

RAICO provides services to healthcare organizations that may involve the processing of Protected Health Information (PHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA). In these cases, RAICO acts as a Business Associate and enters into Business Associate Agreements (BAAs) with covered entities before processing any PHI.

RAICO's obligations with respect to PHI are governed by the applicable BAA, HIPAA, and the HITECH Act. Our privacy and security practices for PHI include:

- Access controls and authentication for all systems that process PHI
- Encryption of PHI in transit and at rest
- Audit trails and logging of all access to PHI
- Incident response and breach notification procedures compliant with HIPAA requirements
- Regular risk assessments and security reviews
- Workforce training on HIPAA privacy and security requirements

RAICO does not use or disclose PHI except as permitted or required by the applicable BAA, HIPAA, or as required by law.

Last updated: April 13, 2026
