

Privacy Policy

CaseSavant — Privacy Policy

Effective Date: pending final legal review

Last Updated: July 8, 2026

1. Introduction

Noya Ventures Inc. ("Noya Ventures," "we," "us," or "our") operates CaseSavant, a legal customer relationship management ("CRM") platform designed for law firms and legal professionals (the "Service"). This Privacy Policy explains how we collect, use, disclose, and safeguard information when you use the Service.

CaseSavant is a business-to-business service. Our direct customers are law firms (each, a "Law Firm"). Individuals interacting with the Service include staff members of Law Firms ("Staff Members") and third parties whose information is stored in the Law Firm's CRM ("Contacts"), which may include the Law Firm's clients, doctors, witnesses, opposing counsel, and other parties involved in the Law Firm's practice.

By using CaseSavant, you agree to the collection and use of information in accordance with this Privacy Policy.

2. Company and Contact Information

- **Legal Entity:** Noya Ventures Inc.
- **Registered Address:** 8215 S Eastern Ave Ste 107, Las Vegas, NV 89123, United States
- **General Inquiries:** support@noyaventures.com
- **Privacy Inquiries and Data Subject Requests:** privacycasesavant@noyaventures.com

3. Roles of the Parties

For purposes of applicable data protection laws:

- **Law Firm as Controller:** With respect to information about the Law Firm's Contacts (including their clients and other parties), the Law Firm acts as the data controller. The Law Firm determines what information to collect from Contacts, how it is used, and for what legal purposes.
- **Noya Ventures as Processor:** With respect to Contact information stored on behalf of Law Firms, Noya Ventures acts as a data processor. We process this information solely on instructions from the Law Firm.

- **Noya Ventures as Controller:** With respect to Staff Member account information (names, emails, credentials, usage data) and Law Firm business information, Noya Ventures acts as a data controller.

4. Information We Collect

4.1 Information You Provide Directly

From Law Firms and Staff Members:

- Business contact information (name, email address, phone number, mailing address)
- Account credentials (username, encrypted password)
- Billing information (routed to our payment processor; see Section 6.3)
- User type and privilege assignments
- Content generated within the platform (case descriptions, notes, communications, uploaded documents)

From Contacts (added by the Law Firm):

- Contact details (name, phone, email, address)
- Case-related information provided by the Contact directly (e.g., through intake forms, digital signatures, or Portal access)
- Any content the Contact submits via the Contact Portal

4.2 Information Collected Automatically

- Usage data (features accessed, actions performed, timestamps)
- Device and browser information (IP address, browser type, device type, operating system)
- Log data (session logs, error logs, security events)
- Essential cookies for authentication and session management

We do not use analytics cookies, marketing cookies, or third-party tracking pixels.

4.3 Information Collected via Integrations

CaseSavant integrates with third-party services at the user's option. When a Staff Member connects an integration, we access data as described below:

Google Workspace Integration:

- **Scopes requested:** `userinfo.email`, `userinfo.profile`, `gmail.modify`, `calendar.events`
- **Data accessed:** Email messages exchanged with Contacts and Staff registered in the Law Firm's CRM; calendar events created or modified by the user
- **Purpose:** To display email correspondence with specific known parties in the CRM, send emails on behalf of the user to those parties, mark emails as read when viewed within CaseSavant, and export calendar appointments to the user's Google Calendar

Microsoft 365 Integration (Outlook & Calendar):

- **Scopes requested:** `openid, profile, email, offline_access, User.Read, Mail.ReadWrite, Mail.Send, Calendars.ReadWrite`
- **Data accessed:** Email messages exchanged with Contacts and Staff registered in the Law Firm's CRM; calendar events
- **Purpose:** Same as Google — display, send, and mark as read emails with known parties; sync calendar appointments

Microsoft 365 Integration (OneDrive/SharePoint):

- **Scopes requested:** `User.Read, Files.ReadWrite`
- **Data accessed:** Files that the user explicitly selects via the official Microsoft File Picker
- **Purpose:** To import user-selected files from OneDrive or SharePoint into specific Matters within CaseSavant. We do not browse, index, or access files that the user does not explicitly select.

4.4 Information Related to Communications

CaseSavant provides voice, SMS, email, video conferencing, and fax capabilities. Information related to communications routed through the platform may include:

- Call metadata (caller, recipient, duration, timestamp)
- SMS content and metadata
- Voicemail and call recordings (when applicable)
- Faxes received on registered fax numbers
- Video session transcripts and AI-generated summaries (Live Sessions module)
- AI-generated call summaries (for calls handled by the Agentic AI)

4.5 Medical Records (Retrieval Process)

The Medical Records module enables Law Firms to obtain medical records via a robotic process automation (RPA) workflow. In this workflow:

- The Law Firm's Contact (patient/client) signs a consent form authorizing the retrieval
- The RPA is executed on the Doctor's own equipment using credentials that the Doctor enters manually
- Retrieved medical records are transmitted to the Law Firm's CaseSavant account

The Medical Records module is not currently offered to Customers for the processing of Protected Health Information as defined under the Health Insurance Portability and Accountability Act ("HIPAA"). Customer use of the module for PHI processing is subject to execution of a separate Business Associate Agreement between the Customer and Noya Ventures. Absent such agreement, Customers shall not use the module in any manner that would result in the processing of PHI through the Service, and remain solely responsible for HIPAA compliance regarding any information they process through the Service.

5. How We Use Information

We use information for the following purposes:

- **Providing the Service:** operating the platform, storing and displaying content, executing user actions, delivering notifications
- **Communications:** sending service-related communications, responding to inquiries, providing support
- **Improvement:** analyzing usage patterns (in aggregate) to improve functionality and performance
- **Security and Fraud Prevention:** monitoring for unauthorized access, protecting the integrity of the platform
- **Legal Compliance:** complying with applicable laws, regulations, and legal requests
- **Billing:** processing payments through our payment processor

5.1 Use of Artificial Intelligence

CaseSavant uses artificial intelligence services provided by Amazon Web Services (specifically AWS Bedrock, Amazon Transcribe, and Amazon Textract) for the following purposes:

- Generating summaries and transcripts of voice calls handled by the Agentic AI (AI Call Summaries)
- Generating transcripts and summaries of Live Sessions (video meetings)
- Powering the AI Assistant that helps users navigate and act within the platform
- Assisting in document generation and processing (e.g., Court Forms, Document Templates)

Data sent to AI services is used solely to provide the requested feature to the user who invoked it. Content processed through AWS Bedrock is not retained by AWS beyond the duration of the request and is not used to train general AI models. Data processing complies with AWS's standard data-handling terms, which prohibit training of AWS's foundation models on customer data.

5.2 Google Limited Use Disclosure

CaseSavant's use of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. Specifically:

- We use Google user data only to provide user-facing features that are prominent within CaseSavant
- We do not transfer Google user data to any third party except as necessary to provide the Service, comply with applicable law, or as part of a merger, acquisition, or sale of assets with user notice
- We do not use Google user data for advertising purposes
- We do not allow humans to read Google user data unless we have the user's affirmative agreement, it is necessary for security purposes, to comply with applicable law, or the data has been aggregated and anonymized

6. How We Share Information

6.1 Sub-Processors

We engage the following third-party sub-processors to provide the Service. Each sub-processor is contractually bound to safeguard user information consistent with this Privacy Policy.

Sub-Processor	Purpose	Location
Amazon Web Services, Inc.	Cloud infrastructure, storage, artificial intelligence processing, email delivery (SES), notifications (SNS), SMS routing (AWS End User Messaging / Pinpoint), monitoring and security	United States
AMCS LLC (Amazon Chime Voice Connector)	Voice telecommunications services (subsidiary of Amazon; provides regulated telecom carrier services)	United States
Elavon, Inc.	Payment processing for Law Firm subscriptions and Client billing	United States
Google LLC	User-authorized integration with Gmail and Google Calendar (only when a Staff Member connects their Google account)	United States
Microsoft Corporation	User-authorized integration with Outlook, Microsoft Calendar, OneDrive, and SharePoint (only when a Staff Member connects their Microsoft 365 account)	United States

6.2 Third-Party Integrations Authorized by the User

When a Staff Member connects their Google or Microsoft account, information flows to those services based on the user's explicit authorization. Information transmitted to Google or Microsoft as part of these integrations is subject to those companies' respective privacy policies.

6.3 Payment Processing

Payments are processed by Elavon, Inc. We do not store full payment card numbers on our servers. Payment card information is transmitted directly to Elavon's PCI-compliant infrastructure.

6.4 Legal Disclosures

We may disclose information when required by law, valid legal process, or when necessary to protect our rights, safety, or property, or that of our users or the public.

6.5 Business Transfers

If Noya Ventures is involved in a merger, acquisition, financing, or sale of assets, information may be transferred as part of that transaction. Users will be notified in accordance with applicable law.

6.6 With Law Firm Authorization

Contact information stored in a Law Firm's account is not shared with other Law Firms or third parties without the Law Firm's authorization.

7. Data Retention

We retain information for as long as necessary to provide the Service and comply with legal obligations.

- **Active accounts:** information is retained for the duration of the Law Firm's subscription
- **Terminated accounts:** upon termination of a Law Firm's account, the Law Firm has thirty (30) days to export its data. After this period, we permanently delete the Law Firm's data from our production systems, subject to legal retention requirements and backup retention policies (backup data is deleted in accordance with our backup rotation schedule, typically not exceeding ninety (90) days)
- **Communications and logs:** communications records (call logs, SMS, emails routed through the Service) may be retained for a longer period as required by applicable law or for legitimate business purposes
- **Aggregated and anonymized data:** may be retained indefinitely for analytical and research purposes

8. Security

We implement industry-standard technical and organizational measures to protect information, including:

- Encryption of data in transit (TLS) and at rest (via AWS Key Management Service)
- Role-based access controls within the platform
- Multi-factor authentication for user accounts (where enabled by the Law Firm)
- Regular security monitoring, logging, and audit trails (AWS CloudTrail, CloudWatch, X-Ray)
- AWS WAF protection against common web attacks
- Regular backups via AWS Backup

Despite these measures, no method of electronic storage or transmission is fully secure. We cannot guarantee absolute security.

9. Your Rights

Depending on your jurisdiction, you may have the following rights regarding your personal information:

- **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 obligations
- **Objection:** object to certain uses of your information
- **Portability:** request a machine-readable copy of your data
- **Withdrawal of consent:** where processing is based on consent, withdraw it at any time

To exercise these rights, contact us at privacycasesavant@noyaventures.com. We will respond within the timeframe required by applicable law.

If your personal information is stored in a Law Firm's account and you are a Contact of that Law Firm (not a Staff Member), please direct your request to the Law Firm directly, as they act as the data controller. We will support the Law Firm in fulfilling valid requests.

10. Revoking Third-Party Integration Access

Users who have connected their Google or Microsoft account to CaseSavant may revoke access at any time:

- **Google:** <https://myaccount.google.com/permissions>
- **Microsoft:** <https://account.microsoft.com/consent>

Revoking access will prevent CaseSavant from accessing your Google or Microsoft data going forward. Data previously imported into your Law Firm's CaseSavant account (for example, emails exported to a Matter's Communication Logs) is not automatically deleted upon revocation and remains subject to the Law Firm's data policies.

11. International Data Transfers

CaseSavant is operated from the United States. If you access the Service from outside the United States, your information will be transferred to and processed in the United States. By using the Service, you consent to this transfer.

12. Children's Privacy

CaseSavant is not directed to individuals under the age of 18. We do not knowingly collect personal information from children under 18. If we become aware that we have collected personal information from a child under 18 without parental consent, we will delete it.

13. California Privacy Rights

If you are a California resident, you have additional 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 (subject to legal exceptions), and the right to opt out of the "sale" or "sharing" of personal information. **We do not sell personal information.** To exercise these rights, contact privacycasesavant@noyaventures.com.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Material changes will be communicated by email to Law Firm administrators or through the Service. The "Last Updated" date at the top of this document reflects the most recent revision.

15. Contact

For any questions about this Privacy Policy or our data practices:

Noya Ventures Inc.

8215 S Eastern Ave Ste 107

Las Vegas, NV 89123, United States

Email: privacycasesavant@noyaventures.com