Applied AI Client Privacy Policy

Effective October 25, 2026 | Version 2026-10-25

Applied AI Partners LLC ("Applied AI," "we," "us," or "our") provides consulting, training, implementation, automation, website and marketing services, and software, including our IQ tools. This policy explains how we handle information about our clients, their authorized users, and the people whose information they entrust to us.

Our privacy commitment

We do not sell, rent, trade, or broker your personal information, your clients' personal information, or confidential client content. We do not disclose that information to advertisers, data brokers, or other businesses to build their own marketing lists, advertise to your clients, or exploit the information for unrelated purposes. We do not share personal information for cross-context behavioral advertising.

We use information to deliver the services you request, protect those services, manage our business relationship, and meet legal obligations. We disclose information only for the limited purposes explained below, including to providers that help deliver the services and to recipients you authorize. Providing a service sometimes requires a provider to process information; this is different from selling information or allowing another business to market to your clients.

Scope and responsibilities

This policy covers our handling of information in connection with Applied AI services and our own websites, client portal, and applications. "Client content" means records, documents, communications, recordings, and other material you provide or direct us to process, including information about your customers, prospects, employees, or other contacts. It also includes transcripts, summaries, search representations, and other outputs derived from that material. We treat nonpublic client content as confidential whether or not it qualifies as personal information.

For account administration, billing, and our own business communications, Applied AI determines how information is used. For client content, you generally determine the purposes of processing, and we act on your documented instructions as a service provider or processor. We do not acquire ownership of client content by processing it.

A website or application we build for your business may need your own privacy notice describing your practices. This policy does not replace that notice, your duties to the people whose information you provide, or a required data processing agreement. A signed service agreement, data processing agreement, or business associate agreement governs the matters it specifically addresses. Additional product notices explain feature-specific practices.

Information we receive

The information involved depends on your services and the features you enable. It may include:

- Account and business information, such as names, business contact details, organization details, authorized users, subscription choices, and agreement records.
- Client content, such as customer and prospect records, insurance and policy information, uploaded files, website submissions, communications, and project materials. Where included in your agreed services, this can also include workforce time, compensation, expense, receipt, and coaching records.

- Audio and related records, such as call or meeting recordings, transcripts, summaries, and participant information when a recording or transcription feature is used.
- Connected-service information, such as email, calendar, CRM, or other records within the permissions and integrations you authorize.
- Billing and transaction information, such as billing contacts, invoices, payment status, and limited payment-method details. Payment providers process payment credentials; our hosted software does not store full card numbers or card security codes.
- Technical information, such as IP address, browser or device information, session identifiers, feature usage, and security or error events. Enabled mobile notifications can also involve a device push token and notification routing information.

We receive information from you, your authorized users, people interacting with your enabled services, connected systems you authorize, and technical interactions with our services. Provide only the information needed for the agreed service.

How we use information

We use information to set up and manage services; perform agreed projects and workflows; store and retrieve records; provide enabled communications and AI features; process payments; respond to support requests; and maintain security and reliability. We also use necessary business records to enforce agreements and comply with law.

We may send our business contacts service updates and, where permitted and consistent with their preferences, information about our services. We do not use your clients' records to build our own marketing lists. Client content is not used to develop unrelated products or create datasets for sale. Any use for service maintenance or troubleshooting is limited to supporting the service provided to you.

Limited disclosures

We limit disclosures to information reasonably needed for the relevant purpose:

- Service providers. Providers may process information for hosting, database and file storage, authentication, communications and push delivery, transcription, AI processing, billing, or other agreed service functions. Providers handling client content on our behalf are subject to contractual confidentiality, security, and use restrictions appropriate to their role. They are not authorized to use client content for their own advertising or to sell it.
- Your authorized recipients. We deliver information to your users according to their access permissions and to recipients or systems you instruct us to use. Examples include sending a message, inviting a meeting participant, publishing material you approve for a website, or connecting your own email, calendar, CRM, accounting, advertising, or signature platform. Those recipients may have their own privacy terms. Your instructions do not authorize us to sell data or use it for our own advertising.
- Legal and safety obligations. We may disclose information when required by law or valid legal process, or as legally permitted to address fraud, security threats, or protect legal rights. We limit the disclosure and notify the affected client where legally permitted and appropriate.
- A business transition. A merger, acquisition, or transfer of the services may involve transferring related records under confidentiality protections. Any successor must honor the applicable privacy and contractual commitments. We provide notices and obtain consent where required. This does not authorize selling client data as a separate asset or permitting unrelated use.

Authorized Applied AI personnel are subject to confidentiality obligations and may access information only as needed for their assigned responsibilities. Our personnel do not browse hosted IQ customer records. Human access to hosted mailbox contents, call recordings, and meeting transcripts for support is limited to what an agency-initiated support request requires, consistent with the applicable product notice. For consulting, implementation, and other custom work, access is limited to the documented client-approved scope. Legally required disclosures remain subject to the limits above; this policy does not expand access permitted by a stricter product notice or agreement.

Our security page at www.appliedaijax.com/security/#subprocessors identifies providers used for hosted IQ services. Contact us for the provider information applicable to your service, including enabled mobile features or connected systems. A custom engagement may have a different approved provider list, which we identify in the project documentation. We explain material new processing arrangements and obtain authorization where required by your agreement or law.

Payment providers may also handle billing and transaction information under their own privacy notices for fraud prevention, financial compliance, and required recordkeeping. This does not authorize Applied AI to sell client content or disclose it for third-party marketing.

AI processing

When an agreed feature uses AI, the information needed for that task may be processed by an approved AI or transcription provider. This can include creating summaries, drafts, transcripts, and search representations used to find your records. Processing content for these tasks does not authorize model training. We do not use client content to train AI models or authorize our providers to use it for model training, and we do not enroll client content in feedback, evaluation, or data-sharing programs that permit that use. We do not enter confidential client content into consumer AI accounts or programs that permit training on submitted content.

Our requirements for approving an AI, transcription, or voice provider to receive client content include applicable commercial terms and account settings that prohibit training on that content and its derived outputs. This requirement includes AssemblyAI and ElevenLabs when used for your services. Where a provider offers a model-improvement or data-sharing program, the applicable account must be excluded from that program before it is approved for client content.

No model training does not mean no retention. Providers may retain limited information for security, abuse prevention, or other operational purposes under their applicable agreements. The relevant product documentation or project terms describe provider-specific limits. AI features and their data flows must be approved for the engagement before sensitive information is submitted.

AI results can contain mistakes and require appropriate human review. We use AI to assist the agreed service; we do not independently use client content to decide a person's eligibility for insurance, credit, employment, or similar opportunities.

Connected services and communications

You choose which external accounts and workflows to enable. Permissions and information exchanged depend on the integration. Email features may involve message bodies, recipients, attachments, and sending or organizing messages; calendar features may involve availability, events, and attendees. Access within your organization follows the product's roles and sharing controls. Depending on the feature, authorized owners, administrators, or teammates may be able to view connected mail or shared records. The connection screen and product notices explain the access that applies.

Our use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including its Limited Use requirements, and applicable Google Workspace user data rules. Google user data is used only for the permitted user-facing features you enable, not for advertising, data brokerage, or model training. Transfers and human access remain limited by those rules.

You can disconnect supported integrations in the service or revoke permission with the connected provider. Disconnecting prevents further authorized syncing; it does not necessarily delete information previously imported or delivered. Some providers require you to revoke a credential separately, such as an Apple app-specific password. Existing records remain subject to applicable retention and deletion rules.

You are responsible for having authority to provide information and for required notices and permissions, including for recording calls or meetings and sending communications. Receipt of this privacy policy is not consent to receive marketing texts or calls. Mobile numbers, SMS opt-in records, and consent information are not sold or disclosed for third-party marketing. Necessary delivery providers may process messaging information to operate the messaging service.

Mobile permissions and device copies

Depending on the app and enabled feature, a native app may request access to the microphone, camera, selected files, or notifications. You control these permissions through the app and device settings. Permission enables the relevant feature and does not authorize unrelated collection. Device recordings, cached records, and exported files can remain on the device separately from our hosted records. Keep your device protected and use the available controls to manage those copies.

Security and data location

We maintain administrative, technical, and organizational safeguards appropriate to the information and service. For our hosted software, these include encryption during transmission and at rest, access controls, and tenant isolation. Multifactor authentication is mandatory for our hosted web applications. Native applications have product-specific authentication requirements described in their notices. We restrict access and require confidentiality for personnel handling client content. No system or transmission can be guaranteed completely secure.

Our hosted IQ service records and files use United States hosting and storage. Provider processing locations and any additional location restrictions are addressed in the applicable service documentation and agreements. For custom work involving your own systems or additional providers, locations and responsibilities are addressed in the engagement documentation. Any agreed restriction on processing location continues to apply. We do not represent that a client's independently selected provider has the same practices as our hosted services.

If a security incident affects client content, we notify affected clients and cooperate with response obligations as required by applicable law and agreement. Any specific contractual notification deadline continues to apply.

Retention and deletion

We retain information for the period needed to provide the relevant service and satisfy applicable legal, security, accounting, or contractual requirements. Retention depends on the type of record, product settings, and any valid legal hold. Recordings, transcripts, project materials, invoices, and account records can have different schedules. Product documentation or your agreement describes any specific retention period that applies.

You may use available export and deletion controls or contact us to request return or deletion of client content. We verify the requester's authority and apply the relevant agreement and legal requirements. Hiding, archiving, or removing an item from a view may retain its underlying record; these actions do not necessarily erase stored information. Ending a subscription or disconnecting an integration also does not necessarily delete all records immediately. We explain applicable exceptions and timing when handling a request.

Backup copies expire under their established retention cycles. While retained, they remain protected and are not used for unrelated purposes. Information that must remain for a legal obligation, valid hold, security, or dispute is limited to that purpose. Copies already delivered to your authorized recipients or connected systems follow those recipients' retention and deletion rules. Native apps may also keep local recordings, cached records, or downloaded files; use the available device or app controls to manage those copies. A request to erase hosted data does not automatically erase a separately retained device copy.

Privacy requests and choices

Contact info@appliedaijax.com or call (904) 830-9969 to ask about our practices or request access, a copy, correction, or deletion of personal information. Depending on your location and the law that applies, you may also have rights to limit certain sensitive-data uses, object to or restrict processing, opt out of targeted advertising or certain profiling, and appeal a denied request. We do not sell personal information or share it for cross-context behavioral advertising.

We verify identity and authority using information appropriate to the request and respond within applicable legal deadlines. An authorized agent may submit a request with proof of authority where permitted. If we deny a request, we explain the reason and any available appeal process. You may appeal by contacting us with your original request details. We do not unlawfully discriminate for exercising privacy rights.

If your information was provided by one of our clients, that client usually directs our handling of it. Please contact that business first. If you contact us, we help route or address your request consistent with our obligations and the client's instructions.

You may unsubscribe from optional marketing email or ask us to stop it. Necessary account, billing, security, and service messages may continue. Requesting deletion or restricting necessary processing may affect our ability to deliver a service.

Cookies and website technology

Our websites and applications use cookies and similar technologies for sign-in, session security, and preferences. Our marketing website also uses Google Analytics to measure visits and interactions, such as page views and use of links or forms. Analytics may involve cookie identifiers, browser or device information, and page or referral information; this is separate from the client records processed in our hosted services. Browsers allow you to manage cookies, and Google provides a browser opt-out tool for Google Analytics. Blocking necessary cookies may prevent sign-in or other features from working. We provide additional choices where required by applicable law. Any analytics, embedded content, or advertising tools used for a client project are described in that project's applicable notices and choices. We do not use client content for our own targeted advertising.

Sensitive information and children

Our general business services are intended for authorized adult users, not for children to sign up independently. We do not knowingly collect personal information directly from children under 13 through our general business services. Tell us if you believe that has occurred. Any engagement involving children's or student information requires a specific assessment, appropriate notices, and any required consents or agreements before collection.

Do not submit protected health information or other specially regulated information unless the service and required written agreements expressly allow it. A general privacy policy alone does not establish HIPAA compliance or replace a business associate agreement. Use approved secure channels for sensitive records.

Changes and contact

We update this policy when our practices or requirements change and identify the effective version. We provide notice of material changes as required by law or agreement and obtain consent where required. A policy update does not authorize us to disregard existing restrictions on previously collected information.

Applied AI Partners LLC • info@appliedaijax.com • (904) 830-9969

Website privacy notice: www.appliedaijax.com/privacy/

Security and provider information: www.appliedaijax.com/security/

Policy version 2026-10-25. Viewing or sharing this policy does not create a signed acknowledgment.