OMNIUS STUDIO LLC d/b/a SOLI

Privacy Policy

Version 1.0 · Effective August 25, 2026 · Omnius Studio LLC d/b/a Soli

Soli Privacy Policy

Effective Date: August 25, 2026 **Last Updated:** 2026-08-14 **Version:** 1.0

Soli is a product line of Omnius Studio, operated by Omnius Studio LLC, a Texas company ("Soli," "we," "us," or "our"). This policy explains what information we collect, why we collect it, who we share it with, how long we keep it, and what choices you have.

We have written this policy to be accurate rather than reassuring. Where our protections have limits, we describe the limits. Where a practice's own obligations govern instead of ours, we say so.

---

1. Scope and Our Role

1.1 Who this policy covers

This policy applies to:

- **Practice customers** — the healthcare practices, clinicians, and businesses that subscribe to Soli Forms or Soli Line;
- **Authorized users** — the owners, administrators, and staff members who hold accounts within a practice's Soli workspace;
- **Visitors** to our websites and to our web chat widget; and
- **Individuals who contact us** for sales, support, or security purposes.

It applies to Soli Forms (our web form builder and intake platform), Soli Line (our business phone line, voicemail, SMS/MMS, fax, and AI receptionist service), and our associated web, desktop, and mobile applications.

1.2 The two roles Soli plays — please read this section carefully

Soli handles two categories of information under two entirely different legal regimes, and the distinction determines which rights apply to which data.

(a) Customer and account data — Soli acts as a controller. This is information about our customers and their authorized users: registration details, billing contacts, authentication records, device and session data, support correspondence, and audit logs. We decide the purposes for which this information is processed. This policy — including the choice and rights mechanics in Sections 10 through 12 — governs that data.

(b) Protected health information processed for a practice — Soli acts as a business associate. When a practice uses Soli to collect intake forms, receive patient calls and voicemail, exchange messages with patients, or operate an AI receptionist, the patient information involved is protected health information ("PHI") that belongs to the practice. We process it **only** on the practice's instructions and **only** as permitted by the Business Associate Agreement ("BAA") executed between Soli and that practice.

> **PHI processed on behalf of a practice is governed by the BAA and by that practice's own Notice of Privacy Practices — not by this policy.** The consumer-choice mechanics in this policy (consent withdrawal, opt-outs, deletion requests, and similar) do not apply to PHI. If you are a patient and you want to access, amend, restrict, or delete your health information, you must contact the practice that treats you. See Section 10.4.

Where this policy and an executed BAA conflict as to PHI, **the BAA controls.**

1.3 What this policy does not cover

This policy does not cover the privacy practices of the practices themselves, of any third-party website that embeds a Soli form, or of any third-party service a practice separately chooses to connect. Those are governed by their own notices.

---

2. Information We Collect

We organize this section by where the information comes from, because the source determines how it is protected and who controls it.

2.1 Account and registration information

When a practice creates an account and adds users, we collect:

- name;
- email address (email verification is required before an account becomes active);
- telephone number;
- practice information, including practice name and the practice-level details needed to provision service;
- the user's role within the practice — `owner`, `admin`, or `member` — and the practice identifier that scopes their access;
- authentication records, including credentials managed by our identity provider, and identifiers issued by an external identity provider where a user signs in through Google or Microsoft single sign-on;
- multi-factor authentication enrollment data, including time-based one-time password (TOTP) registration, recovery codes, and WebAuthn/passkey credentials.

Authentication is operated through Firebase Authentication / Google Cloud Identity Platform. Passwords are hashed by that service; we do not receive or store passwords in readable form. We do not use SMS one-time codes for authentication.

2.2 Billing information

Subscription billing is processed by **Stripe**. Stripe collects and processes payment card details directly. **Soli does not receive or store full payment card numbers.** We retain the billing contact information and subscription records associated with an account — such as the billing contact's name and email address, plan, and transaction history — for accounting and support purposes. Billing records are not intended to contain PHI, and practices should not place patient information in billing fields.

2.3 Customer Data — form submissions and telephony content

"Customer Data" means the content a practice and its patients place into the services. It includes:

- form submissions collected through Soli Forms, and any file attachments and electronic signatures included with them;
- voice call content, voicemail recordings, call transcripts, SMS/MMS message bodies, and fax content handled through Soli Line;
- messages exchanged through the Soli web chat widget; and

- contact records a practice maintains within the services.

Customer Data belongs to the practice. For covered entities, it is generally PHI. Section 3 describes precisely how it is encrypted, including the points at which encryption does and does not apply.

Certain contact fields associated with a submission — specifically a patient's name, email address, and telephone number stored in the `safe_contact` record — are encrypted on our servers using managed key material as described in Section 3.4.

Telephone numbers appearing in call and message logs are stored as **HMAC-SHA256 hashes** computed with a server-side secret value, rather than as encrypted values, so that the logs remain searchable. A hash of this kind is a pseudonymized identifier, not anonymous data: the same number always produces the same hash, and anyone holding the secret value could confirm whether a particular number appears in a log.

2.4 Information collected automatically

When you use the services we automatically collect:

- **Device and session information** — browser and application version, operating system, device type, and session identifiers, used to maintain your session and to detect abuse;
- **Network identifiers in hashed form** — IP addresses and user-agent strings associated with security-relevant events are stored as **hashes**, not in plaintext, in our audit records;
- **Audit logs** — an append-only record of security-relevant activity, scoped to each practice, capturing the actor, the action, the resource affected, and the timestamp. Audit logs deliberately record *that* PHI was accessed or decrypted; they do **not** record the PHI values themselves. Our production logging pipeline is configured to redact common sensitive fields, including email address, telephone number, name, Social Security number, medical record number, date of birth, address, and authentication tokens;
- **Application diagnostics** — error and performance data used to keep the services running. The Soli Forms form-hosting service does not log request bodies, so submitted form content does not enter those logs.

2.5 Mobile application permissions

The Soli Line mobile application requests the following operating-system permissions. Each is optional at the OS level, and declining a permission disables only the corresponding feature.

Permission	Why it is requested	What leaves the device
Contacts (read-only)	To match incoming calls and messages against your device contacts and display familiar names	**Nothing.** Contact matching happens locally on the device. Your contact list is not uploaded to Soli.
Microphone	To place and receive calls and to record outgoing voice messages	Call audio, as described in Sections 3.2 and 5
Camera and photo library	To attach images and documents to messages	Only the files you choose to attach
Biometric authentication (Face ID / Touch ID / equivalent)	To unlock the app and release the locally stored encryption key from the OS keychain	**Nothing.** Biometric data never leaves your device and is never accessible to Soli; the OS returns only a success or failure signal.

Push notifications sent to the mobile application **contain no PHI**. The notification payload is limited to a message type, a line identifier, and an envelope identifier; the application decrypts and displays the underlying content locally on the device after you open it.

2.6 Information we do not seek

We do not ask practices or patients to provide government identification numbers, precise geolocation, or biometric identifiers to Soli, and we do not collect them for our own purposes. Practices may, of course, design forms that request such information from their own patients; that content is Customer Data under Section 2.3 and is governed by the practice's BAA.

---

3. Encryption and Zero-Knowledge Design

Soli is built so that, for most Customer Data, our servers hold ciphertext they cannot read. We describe the design specifically below, including its boundaries, because a general assurance of security would tell you nothing useful.

3.1 Soli Forms — client-side encryption

Form submissions are encrypted **in the patient's browser, before they are transmitted to us**, using the libsodium sealed-box construction (`crypto_box_seal`) against the public key of each recipient the practice has authorized. Soli's servers never receive the plaintext submission.

File attachments are encrypted in the browser with a randomly generated per-file symmetric key; that key is itself sealed to each authorized recipient's public key, and the encrypted file is uploaded to storage through a signed URL. The service that renders and encrypts forms is a stateless proxy — it has no database of its own, and it does not log request bodies.

3.2 Soli Line — line-scoped encryption

Telephony content is encrypted with a key scoped to the individual phone line, using an X25519 sealed box. The private key for a line is wrapped separately for each authorized team member using a key derived from that member's password (PBKDF2, 600,000 iterations, SHA-256) and stored as an opaque blob. **Soli's servers cannot unwrap the line private key**, and therefore cannot read line-encrypted content.

An important limitation. Inbound SMS bodies and call content arrive at our servers **in plaintext** at the point where our telecommunications provider delivers them to us. We encrypt that content in memory immediately on receipt and discard the plaintext; it is not written to disk in readable form. But the content does exist in plaintext transiently within our systems at that boundary, and — as Section 5.2 explains — it has already been processed by our telecommunications provider before it reaches us. Our encryption model protects data at rest on Soli's infrastructure. It does not, and cannot, retroactively protect content that a provider handled upstream of us.

3.3 Metadata is not encrypted

Message and call timestamps, direction, duration, line identifiers, message counts, and similar operational metadata are stored unencrypted so the services can function. Telephone numbers in logs are hashed as described in Section 2.3. Metadata about communications with a healthcare practice can itself be sensitive, and we treat it as PHI under the BAA, but you should understand that it is not covered by the zero-knowledge design.

3.4 Server-side field encryption with managed keys

The `safe_contact` fields — patient name, email address, and telephone number — are encrypted using **Google Cloud KMS envelope encryption** before they are written to our database, with automatic key rotation on a 90-day cycle. If the key management service is unavailable, submissions **fail closed** with an error; there is no plaintext fallback path.

Because these fields are encrypted with keys we manage rather than keys only the practice holds, they are not zero-knowledge. We distinguish them from Sections 3.1 and 3.2 for that reason.

3.5 Encryption on your devices

- **Desktop (Soli Forms for Windows/macOS/Linux):** data is stored in a local SQLite database in the application's user-data directory, with sensitive columns encrypted using **AES-256-GCM**. The master key is held in the operating system keychain and never leaves the device.
- **Mobile (Soli Line):** message bodies are stored in the local database only in encrypted form (**AES-256-GCM**). Voicemail audio is decrypted in memory for playback and is never written to disk in plaintext. The encryption key is held in the OS keychain and is released under the device's own lock or biometric protection.

3.6 Transport security

All connections between your devices and our services use TLS. All data at rest on our cloud infrastructure is additionally encrypted by the platform, beneath the application-layer encryption described above.

3.7 What zero-knowledge does not mean

To be explicit about the boundaries of this design:

1. It does not apply to account, billing, or metadata described in Sections 2.1–2.4.
2. It does not apply to content while it is held by, or being processed by, our telephony and AI subprocessors (Sections 5.2 and 6).
3. It does not prevent an authorized user of a practice from reading Customer Data — that is the point of the product.
4. If a practice loses all copies of a line's private key material, we cannot recover the affected content. That is a direct consequence of the design.

---

4. How We Use Information

We use information for the following purposes and no others:

- **To provide the services** — provisioning accounts and phone numbers, delivering and routing calls, messages, faxes, and form submissions, storing and synchronizing encrypted content, and operating scheduling, telehealth, and AI receptionist features a practice has enabled.
- **To authenticate users and secure the services** — verifying identity, enforcing multi-factor authentication, applying rate limits, detecting and investigating abuse or unauthorized access, and maintaining audit records.
- **To provide customer support** — responding to inquiries and diagnosing problems. Support access to a practice's environment is logged.
- **To bill for the services** — processing subscriptions and payments through Stripe, and handling invoices, taxes, and collections.

- **To communicate with you** — sending transactional, service, security, and billing notices, and (where permitted, and subject to opt-out) product announcements to account contacts.
- **To comply with law** — meeting legal, regulatory, tax, and telecommunications obligations, and responding to lawful requests as described in Section 5.4.
- **To improve and secure the product** — using aggregate operational and diagnostic data, and de-identified or aggregated usage statistics, to diagnose faults, plan capacity, and improve reliability and features.

4.1 Commitments about PHI, AI training, and sale of data

- **We do not use PHI to train, fine-tune, or otherwise improve artificial intelligence or machine learning models**, whether our own or a third party's. AI processing of Customer Data occurs only to deliver a feature the practice has enabled, at the time it is used. Section 6 describes that processing.
- **We do not sell Customer Data, and we do not sell personal information.** We do not share personal information for cross-context behavioral advertising. See Section 11.
- **We do not use Customer Data for advertising**, and we do not disclose it to advertising networks or data brokers.
- **We do not access decrypted Customer Data except as necessary** to provide the services, to respond to a practice's support request, or as required by law. Where a decryption event occurs, it is recorded in the practice's audit log.

---

5. How We Disclose Information

We disclose information only in the circumstances described below. A current list of our subprocessors — the vendors that process data on our behalf — is published alongside this policy as **the Subprocessor List** and is available to customers on request. We will provide advance notice of material changes to that list in accordance with the terms of the applicable customer agreement and BAA.

5.1 Cloud infrastructure

All Soli services are hosted on **Google Cloud Platform**, which provides our compute, primary database, file and backup storage, key management, secret storage, logging, and task queueing, as well as the identity platform used for authentication. Google Cloud may hold PHI in the course of providing that infrastructure. **We maintain a signed Business Associate Agreement with Google Cloud**, and we use services within Google Cloud's HIPAA-eligible scope for this purpose.

5.2 Telecommunications and telephony processing — Telnyx

Soli Line is delivered using **Telnyx**, our telecommunications provider. Telnyx provisions telephone numbers and carries voice, SMS/MMS, and fax traffic. In addition, and importantly:

- **Voicemail recording.** When a caller leaves a voicemail, the recording is made and stored on Telnyx infrastructure, and Soli subsequently retrieves it, encrypts it, and stores it. **The recording exists on Telnyx systems before Soli encrypts it.**
- **Transcription.** Speech-to-text transcription of call and voicemail audio is performed by Telnyx.
- **AI receptionist.** Where a practice enables the AI receptionist, live call audio is streamed to Telnyx for speech recognition, language-model processing, and speech synthesis. See Section 6.
- **Inbound messages.** The text of inbound SMS and MMS messages is delivered to Soli in Telnyx's webhook payload, which means Telnyx has processed the message content.

Telephony content handled through Soli Line — including call audio, voicemail recordings, transcripts, and message content — is therefore processed by our telecommunications provider, and that content may constitute protected health information. We state this plainly because any suggestion that patient content does not reach our telecommunications provider would be inaccurate. Practices evaluating Soli Line for use with patients should take this into account, and should raise it with us and with their own compliance advisors.

5.3 Other subprocessors

Category	Purpose	Data involved
Payments (Stripe)	Subscription billing and payment processing	Billing contact and transaction data. Not intended to include PHI. Full card numbers are held by the processor, not by Soli.
Transactional email and calendar (Microsoft 365 / Microsoft Graph)	Sending service email; calendar integration where a practice connects it	Message recipients and message content. Email bodies sent on a practice's behalf may contain PHI.
Real-time media relay (Metered)	TURN/STUN relay for telehealth sessions	Relayed media streams. The relay carries session media; it does not store session content.
Malware scanning (ClamAV)	Scanning uploaded files before storage	File content is processed in unencrypted form at the moment of scanning.
AI inference providers	Transcription, summarization, AI receptionist, and AI-assisted form-field generation	See Section 6.

5.4 Other disclosures

- **Within a practice.** Customer Data is available to the authorized users of the practice that owns it, according to the roles the practice assigns.
- **At the practice's direction.** We disclose Customer Data to third parties when a practice instructs us to, including through integrations the practice enables.
- **Legal process and safety.** We may disclose information where required by law, subpoena, warrant, court order, or other lawful process, or where necessary to protect the rights, property, or safety of Soli, our customers, or the public. For PHI, we follow the notice, objection, and minimum-necessary requirements of the BAA and of 45 C.F.R. Part 164, and we will notify the affected practice of a legal demand for its data unless we are legally prohibited from doing so.
- **Corporate transactions.** If Soli is involved in a merger, acquisition, financing, or sale of assets, information may be transferred as part of that transaction. Any recipient of PHI would be required to assume the obligations of the applicable BAA, and we will provide notice of any such transfer.
- **Professional advisors.** We disclose information to our auditors, insurers, and legal counsel under duties of confidentiality.

We do not disclose Customer Data to any other party.

---

6. Artificial Intelligence Processing

Several Soli features are delivered using artificial intelligence, and we want this to be unambiguous rather than buried.

Call audio, voicemail recordings, transcripts, and chat messages may be processed by AI systems. Specifically:

- **Transcription.** Call and voicemail audio may be converted to text by an automated speech-recognition system operated by our telecommunications provider, Telnyx.
- **AI receptionist.** Where a practice enables it, live call audio is streamed to an AI system that performs speech recognition, generates a response using a large language model, and synthesizes speech. **This AI receptionist runs on inference infrastructure hosted by Telnyx**, our telecommunications provider, using a third-party open-weight language model selected by Soli. Callers are told at the start of the call that they are speaking with an AI.
- **Summarization.** Transcripts and message threads may be summarized automatically for the practice's review.
- **Web chat.** Messages sent through the Soli web chat widget are processed by an AI system in order to generate replies. The widget displays a notice asking visitors not to share sensitive health information and directing emergencies to 911. **That notice is a warning, not a technical restriction.** Nothing prevents a visitor from entering health information, and if a visitor does so, Soli receives and processes it. Please do not use the chat widget to communicate health information or in an emergency.
- **AI-assisted form building.** When a practice uses AI assistance to generate or refine form fields, the prompt content is sent to a third-party AI provider (currently OpenAI and/or Google Gemini services). This feature is intended for use with form design content, not with patient data.

Content processed by these systems is used solely to produce the output the feature requires. **It is not used to train or improve AI models.**

---

7. Data Retention

The periods below are **maximum default retention windows**, not guarantees of the exact moment of deletion. Where our deletion is delayed or requires manual action, we say so.

Category	Retention
Encrypted submission envelopes, form submissions, and encrypted file blobs	**30 days by default**, after which they are scheduled for automatic deletion. Encrypted blobs in object storage are removed by a 30-day lifecycle rule.
Automatic deletion lag	Scheduled deletion is **eventual, not immediate**. Records may persist for **up to 72 hours** after their expiry time before they are actually removed.
Audit logs	**6 years**, consistent with HIPAA documentation-retention requirements. Audit logs record access events and never PHI values.
Backups	Daily database exports are held on a **30-day rolling retention**, with monthly archives retained for **6 years**. Data deleted from live systems persists in backups until the applicable backup expires.
Account and billing records	Retained for the life of the account and thereafter as required for tax, accounting, and legal purposes.
Encrypted content held on your devices	Retained locally until you delete it or remove the application.

Deletion requests and their limits. A practice may submit an account deletion request through the application. We want to be candid about how this currently works: **the request is recorded and then acted on through a manual process.** We do not currently operate a fully automated cascade deletion that purges every related record on a fixed

timetable, and we therefore do not promise a specific completion interval. We will confirm to the practice when deletion has been carried out. Data already written to backups is removed as those backups expire on the schedule above, and is not selectively purged from existing backup media.

At termination of a BAA, we return or destroy PHI in accordance with the terms of that BAA. Where return or destruction is infeasible, we extend the protections of the BAA to the retained information and limit further use and disclosure to the purposes that make destruction infeasible.

---

8. How We Protect Information

In addition to the encryption described in Section 3:

- **Authentication.** Email verification is required. We support **TOTP multi-factor authentication** with recovery codes and **WebAuthn passkeys**. We do not use SMS one-time codes, which are the weakest widely deployed second factor.
- **Access control.** Role-based access control assigns each user the `owner`, `admin`, or `member` role within their practice, and access rights follow from that role.
- **Tenant isolation.** Every record is partitioned by practice identifier, and that partition is enforced in application middleware and in every query path.
- **Audit logging.** Security-relevant events, including decryption of protected content, are written to an append-only per-practice audit log.
- **Session controls.** The application applies a **15-minute idle timeout** in the client, after which the session is ended. Session tokens have a configurable lifetime not exceeding seven days.
- **Rate limiting.** Authentication endpoints are rate limited (30 requests per minute for password login, 15 per minute for passkey authentication) to frustrate credential-guessing attacks.
- **Infrastructure.** The services run on **HIPAA-eligible Google Cloud infrastructure under a signed Business Associate Agreement with Google Cloud**, with platform-level encryption at rest, managed key rotation, and secrets held in a managed secret store.
- **Resilience.** We maintain daily backups with cross-region replication and object versioning, and a documented disaster-recovery objective of restoring service within **72 hours** (recovery time objective).
- **Minimization in logs.** Production logging redacts common identifiers, and IP addresses and user agents in audit records are stored hashed.

No method of transmission or storage is perfectly secure. The controls above reduce risk; they do not eliminate it. We do not represent or warrant that the services or any information within them are immune from compromise, and you should not rely on any single control as absolute protection. Security is also shared: a practice's own password hygiene, device security, staff access management, and offboarding practices materially affect the security of its data.

If you believe you have found a security vulnerability in a Soli product, please report it to **support@meetsoli.com**. We ask that you give us a reasonable opportunity to remediate before public disclosure, and we will not pursue legal action against good-faith security research conducted in accordance with that request.

---

9. Where Information Is Stored

Soli's services are hosted in data centers located in the **United States**, and Customer Data and account data are stored in the United States. Certain subprocessors may operate support or network functions from other locations; a current description is maintained in the Subprocessor List.

Soli's services are offered to healthcare practices operating in the United States. **We do not currently offer a data-transfer mechanism for personal data originating in the European Economic Area, the United Kingdom, or Switzerland** — we do not currently rely on Standard Contractual Clauses or the EU-U.S. Data Privacy Framework, and we do not represent that our processing satisfies the GDPR. If you are subject to those regimes and require such a mechanism, contact support@meetsoli.com before using the services. For customers who require a data protection contact, inquiries may be directed to privacy@meetsoli.com.

If you access the services from outside the United States, you do so on your own initiative and you understand that your information will be transferred to and processed in the United States.

---

10. Your Rights and Choices

10.1 Rights available to account holders and users

Subject to verification of your identity, you may:

- **Access** the personal information we hold about you as an account holder or authorized user;
- **Correct** inaccurate account information, much of which you can update directly in the application's account settings;
- **Delete** your user account, and — if you are a practice owner — request deletion of the practice account, subject to the limitations disclosed in Section 7;
- **Export** your data. Practices can export their Customer Data from the application. Because Customer Data is encrypted to keys the practice holds, export must be performed by an authorized user of the practice using their own credentials; **Soli cannot generate a decrypted export on a practice's behalf**;
- **Object to or restrict** certain processing, and **withdraw consent** where we rely on consent;
- **Opt out of marketing email** using the unsubscribe link in any such message. You cannot opt out of transactional, security, and billing notices while your account is active.

10.2 How to exercise these rights

Email **support@meetsoli.com** with your request and the account it concerns, or use the account controls in the application. We will acknowledge your request and respond within the period required by applicable law. We may need to verify your identity — typically by confirming control of the account email address — before acting, and we may decline requests that are unfounded, excessive, or that would compromise another person's rights.

We do not charge for exercising these rights and we do not discriminate against anyone who does. See Section 11.4.

10.3 Authorized agents

An authorized agent may submit a request on your behalf where state law permits. We require written proof of the agent's authorization and may require you to verify your identity with us directly.

10.4 Patients: how to exercise rights in your health information

If you are a patient of a practice that uses Soli, contact that practice, not Soli. Under HIPAA, your rights of access, amendment, accounting of disclosures, restriction, and confidential communications run against the practice as the covered entity. The practice's Notice of Privacy Practices explains how to make those requests.

Soli holds your health information only as a business associate, in encrypted form, and generally cannot read it. If you send us a request concerning your health information, **we will refer it to the relevant practice** and notify you that we have done so; we will not act on it directly except on the practice's instruction and as the BAA permits.

---

11. California Privacy Rights (CCPA/CPRA)

This section applies to California residents and supplements the rest of this policy. It describes our handling of personal information as a **business** — that is, the account and website data described in Sections 2.1, 2.2, and 2.4.

PHI processed by Soli as a business associate is exempt from the CCPA under Cal. Civ. Code § 1798.145(c), as is medical information governed by the Confidentiality of Medical Information Act. Requests concerning that information should go to the practice, as described in Section 10.4.

11.1 Categories of personal information collected and disclosed

In the preceding twelve months we have collected the following categories, each for the business purposes described in Section 4, and disclosed each to the service-provider categories described in Section 5:

CCPA category	Examples we collect	Source	Disclosed to
Identifiers	Name, email address, telephone number, account and identity-provider identifiers, hashed IP address	You and your practice; automatically	Cloud infrastructure, payments, email, telephony service providers
Customer records information (Cal. Civ. Code § 1798.80(e))	Billing contact and transaction records	You; payment processor	Payments, cloud infrastructure
Commercial information	Subscription plan, purchase and service-usage history	Automatically; payment processor	Payments, cloud infrastructure
Internet or network activity	Device, browser, and session data; application diagnostics; audit-log events	Automatically	Cloud infrastructure
Professional or employment information	Practice name, your role within the practice	You and your practice	Cloud infrastructure
Audio and electronic information	Call and voicemail audio and message content handled through Soli Line	Callers and practices	Cloud infrastructure, telephony provider (see Section 5.2)
Inferences	None. We do not create profiles or infer characteristics about individuals.	—	—

We do not collect biometric information, precise geolocation, or education information for our own purposes.

11.2 Sensitive personal information

We collect one category of sensitive personal information for our own purposes: **account log-in credentials** (in combination with the credentials or security information permitting account access). We use it only to authenticate users and secure accounts.

Health information handled through the services is **sensitive personal information** in character, but where it is PHI it falls within the HIPAA exemption above. Where health-related information reaches us outside HIPAA's perimeter — for example, information a website visitor types into our web chat widget — see Section 12.

We use and disclose sensitive personal information only for the purposes permitted by Cal. Civ. Code § 1798.121(a) and its implementing regulations, and we do not use it to infer characteristics about you. Because our use is limited to those permitted purposes, we are not required to offer, and do not offer, a separate "Limit the Use of My Sensitive Personal Information" control.

11.3 No sale or sharing

We have not sold personal information, and we have not shared personal information for cross-context behavioral advertising, in the preceding twelve months, and we do not do so today. We have no actual knowledge of selling or sharing the personal information of consumers under 16 years of age.

11.4 Your California rights

You have the right to know, to access, to delete, to correct, to obtain a portable copy, to opt out of sale or sharing (which does not apply, as we do neither), to limit the use of sensitive personal information (see Section 11.2), and **not to receive discriminatory treatment** for exercising any of these rights. We do not deny goods or services, charge different prices, or provide a different level of service because you exercised a privacy right.

Exercise these rights as described in Section 10.2. Authorized agents may act for you as described in Section 10.3. If we decline a request, you may appeal by replying to our response; we will explain the outcome in writing.

11.5 Other state privacy laws

Residents of other states with comprehensive privacy laws — including Colorado, Connecticut, Virginia, Utah, Texas, Oregon, and Montana, among others — have comparable rights of access, correction, deletion, portability, and appeal, and comparable exemptions for PHI and for information processed by a business associate. We honor those rights through the same process described in Section 10.2. Where a state law provides a right to appeal a denial, you may appeal by writing to support@meetsoli.com.

---

12. Consumer Health Data (Washington, Nevada, and Similar Laws)

Some state laws protect **consumer health data** more broadly than HIPAA does, and they reach health-related information that falls outside HIPAA's perimeter. This section addresses those laws, principally the **Washington My Health My Data Act** and **Nevada SB 370**. This section serves as our consumer health data privacy notice for those purposes.

12.1 What it covers, and what it does not

Information that Soli processes as a business associate on behalf of a covered entity is **PHI**, and is excluded from these statutes. This section is therefore directed at the narrower set of health-related information that may reach Soli **outside** a HIPAA relationship — most significantly, information a member of the public voluntarily types into the Soli

web chat widget on a practice's website before any treatment relationship exists, and health-related information a person may include when contacting us directly.

12.2 What we collect, why, and with whom we share it

- **Categories collected:** health-related information a consumer chooses to provide in a chat message or in correspondence with us; and the technical data in Section 2.4 associated with that interaction.
- **Purpose:** solely to deliver the message to the practice the consumer contacted, to generate an automated reply where the practice has enabled that feature, and to keep the service secure.
- **Sources:** the consumer.
- **Shared with:** our cloud infrastructure provider and the AI systems described in Section 6, and the practice the consumer contacted.
- **We do not sell consumer health data.** Washington and Nevada law prohibit selling consumer health data without a valid, signed authorization. We do not sell it, and we therefore do not seek such authorizations.
- **We do not operate geofences** around any healthcare facility, and we do not use location data to identify visits to healthcare facilities. Washington and Nevada law prohibit that practice.

12.3 Your rights under these laws

If you are a Washington or Nevada consumer, you have the right to **confirm** whether we collect, share, or sell your consumer health data and to access it; to obtain a **list of third parties** with whom we have shared it; to **withdraw consent** to its collection and sharing; and to have it **deleted**, including from our archives and backups, subject to the backup-expiry limitation disclosed in Section 7. Exercise these rights by writing to support@meetsoli.com. We will respond within the statutory period and will not discriminate against you for exercising them.

Washington residents may also have a private right of action under the Washington Consumer Protection Act for violations of the My Health My Data Act.

12.4 Please do not send health information through the chat widget

Because the web chat widget is a general-purpose, AI-assisted contact channel that operates before any treatment relationship exists, we ask again that you not use it to describe health conditions, and never in an emergency. **In an emergency, call 911.**

---

13. HIPAA and Our Business Associate Relationship

When a practice that is a HIPAA covered entity uses Soli to create, receive, maintain, or transmit PHI, **Soli acts as that practice's business associate** within the meaning of 45 C.F.R. § 160.103.

- **We execute a BAA with every covered-entity customer** before PHI is processed. The BAA governs our permitted uses and disclosures of PHI, our safeguard obligations, our breach-notification obligations, the flow-down of obligations to subcontractors, and the return or destruction of PHI on termination. A copy of our standard BAA is available at support@meetsoli.com or through the account portal.
- **We use and disclose PHI only as the BAA permits** and as required by law, and we apply the minimum necessary standard.
- **We notify the practice of any breach of unsecured PHI** without unreasonable delay and within the timeframe the BAA specifies, so that the practice can meet its own notification obligations.

- **Our subcontractors that handle PHI are required to provide equivalent protections.** Section 5 identifies the categories involved, and the Subprocessor List identifies the specific vendors and their status.

We describe our infrastructure as **HIPAA-eligible Google Cloud infrastructure operating under a signed Business Associate Agreement with Google Cloud**. We deliberately avoid describing any product as "HIPAA compliant" without qualification: HIPAA compliance is a property of an organization's overall program — including the practice's own policies, workforce training, risk analysis, and configuration choices — and not a certification that attaches to software. Where we make a specific security or compliance representation, we maintain documentation supporting it.

---

14. Children's Privacy

The Soli services are business tools intended for healthcare practices and their staff. **They are not directed to children, and we do not knowingly collect personal information directly from children** for our own purposes. Account holders and authorized users must be adults and must be authorized by the practice.

Practices do use Soli to collect and communicate information about **minor patients**. That information is Customer Data and PHI, processed on the practice's behalf under the BAA. **The practice — not Soli — is responsible for obtaining any parental or guardian consent or authorization required** by HIPAA, by state law, or by the Children's Online Privacy Protection Act, and for determining what information about a minor may be collected, disclosed, or disclosed to a parent under applicable state minor-consent rules. Requests concerning a minor patient's information must be directed to the practice.

If you believe a child has provided personal information directly to Soli outside of a practice relationship, contact support@meetsoli.com and we will delete it.

---

15. Cookies, Session Storage, and Tracking

15.1 In the Soli applications

The Soli web application uses **browser session storage** to hold your authentication token for the duration of your session, and uses cookies and equivalent local storage that are **strictly necessary** to operate the service — maintaining your signed-in session, enforcing the idle timeout, protecting against cross-site request forgery, applying rate limits, and remembering interface preferences such as your practice selection.

We do not use advertising cookies, third-party tracking pixels, or cross-context behavioral advertising technology within the Soli applications.

The Soli Forms embedded form widget is served by a stateless rendering service that maintains no database and does not log request bodies. It sets only what is required to render and submit the form.

Because these technologies are strictly necessary to deliver a service you have requested, we do not present a consent banner for them within the application. You can block or delete cookies through your browser, but doing so will prevent you from signing in.

15.2 Do Not Track

We do not respond to browser Do Not Track signals, because no common standard for them has been adopted. Where required by law, we honor recognized opt-out preference signals such as **Global Privacy Control** as a request to opt out of sale or sharing — which, as stated in Section 11.3, we do not engage in.

---

16. Changes to This Policy

We may update this policy as our services, our vendors, or the law change. When we do:

- we will revise the **Last Updated** date and the version number at the top of this policy;
- we will maintain the prior version so that changes can be compared; and
- where the change is **material** — for example, a new category of information collected, a new purpose of use, a new category of disclosure, or a change to a subprocessor that handles PHI — we will provide advance notice to account owners by email and, where practicable, an in-application notice **at least 30 days before the change takes effect**, unless a shorter period is required by law or by an urgent security need.

Changes to our handling of PHI are additionally governed by the BAA, including any notice and consent requirements it imposes. Continued use of the services after a change takes effect constitutes acceptance of the revised policy, except where applicable law requires your affirmative consent.

---

17. Contact Us

Purpose	Contact
Privacy questions, rights requests, and this policy	**support@meetsoli.com**
Security vulnerability reports and suspected incidents	**support@meetsoli.com**
Business Associate Agreements, legal notices, and legal process	**support@meetsoli.com**
Data protection contact	**privacy@meetsoli.com**

Omnius Studio LLC 5900 Balcones Drive, STE 100, Austin, TX 78731

Soli is a product line of Omnius Studio.

If you are a patient with a question about your health information, please contact the healthcare practice that treats you. See Section 10.4.

If you are not satisfied with our response to a privacy request, you may lodge a complaint with your state attorney general. Complaints about the handling of protected health information may also be filed with the U.S. Department of Health and Human Services, Office for Civil Rights, at https://www.hhs.gov/ocr/complaints. We will not retaliate against anyone for filing a complaint.