

Privacy Policy

Palmyra · Effective [EFFECTIVE DATE] · <https://palmyra.life/privacy>

[PALMYRA LEGAL ENTITY NAME], a [STATE OF FORMATION] [ENTITY TYPE, e.g. corporation or limited liability company] ("Palmyra", "we", "us" or "our"), provides software to dental practices, including an AI phone receptionist that answers a practice's calls, and a web dashboard at <https://app.palmyra.life> where practice staff manage calls, messages, settings and billing. This Privacy Policy explains how we collect, use, disclose and protect personal information when you visit our website at <https://palmyra.life>, ask us about early access, or use the dashboard as a member of a dental practice's team. It also explains, in Section 2, how we handle patient and caller information when we act for a dental practice.

Our service is offered only in the United States, to businesses. Our customers are dental practices and dental service organizations (each a "**Practice**"), not individual consumers.

In short:

- Call information belongs to the Practice. We handle it as the Practice's service provider and HIPAA business associate. Patients should send privacy requests to their dental practice.
- We do not sell personal information, "share" it for cross-context behavioral advertising, or use it for targeted advertising, and we do not use protected health information to train AI models.
- Our website sets no cookies and uses no analytics or advertising trackers. Our dashboard uses only the cookies needed to keep you signed in.

1. Scope of this Privacy Policy

This Privacy Policy applies to personal information that we collect and decide how to use in our own right, as a "business" or "controller" under US state privacy laws. That includes information about:

- **Website visitors:** people who visit <https://palmyra.life> and any page that links to this Privacy Policy;
- **Prospects:** people who give us their contact details, for example through our early-access form or by email;
- **Practice users:** owners, administrators and staff a Practice invites to use the dashboard at <https://app.palmyra.life> (together with the website and the AI receptionist, the "**Service**"), including billing contacts and people who contact our support team.

This Privacy Policy does **not** govern information we process on behalf of a Practice, such as information about patients and other callers ("**Practice Data**"). Section 2 explains how that information is handled; for Practice Data, Section 2 and our agreements with the Practice control. Our Terms of Service (<https://palmyra.life/terms>) and Website Terms of Use (<https://palmyra.life/website-terms>) also apply.

2. Patient and caller information: we act for the dental practice

When a patient or anyone else calls a dental practice that uses Palmyra, the AI receptionist may answer the call, talk with the caller, look up or book appointments, answer questions using information the Practice has configured, take a message or voicemail, record requests for a callback, prescription refill or new-patient intake, and transfer the call to the Practice's staff. To do this, the Service processes information such as:

- live call audio and, if the Practice turns recording on, call recordings;
- transcripts, AI-generated call summaries, voicemails, messages and callback requests;
- the caller's phone number and caller ID, patient names, dates of birth and appointment details;
- insurance carrier and plan details, prescription refill requests and new-patient intake answers;
- a short history of summaries of the caller's prior calls, so the AI receptionist can provide continuity; and
- the Practice's configuration, such as hours, locations, providers and FAQs.

2.1 The Practice is in charge of this information

For Practice Data, the Practice decides why and how the information is used, and we act only on the Practice's behalf and according to its instructions. Under the Health Insurance Portability and Accountability Act of 1996 and its regulations ("**HIPAA**"), the Practice is the "covered entity" and Palmyra is its "business associate". Much of the Practice Data is "protected health information" under HIPAA. Under US state privacy laws, we act as the Practice's "service provider" or "processor".

Our handling of Practice Data is governed by our agreements with the Practice, including our Terms of Service (<https://palmyra.life/terms>) and our Business Associate Agreement (<https://palmyra.life/baa>), which every Practice must accept before using features that involve protected health information. How the Practice itself uses and discloses your health information is described in the Practice's own **Notice of Privacy Practices**, which you can get from the Practice.

In particular, for Practice Data:

- we use and disclose it only to provide the Service to the Practice, for our proper management and administration, and as otherwise permitted by our Business Associate Agreement and HIPAA;
- we do not sell it, use it for advertising, or use it to market to callers. Palmyra does not send marketing calls or text messages to patients;
- we do not use protected health information to train AI models; and
- we use subcontractors that handle protected health information only under written agreements that require them to protect it as HIPAA requires.

2.2 How to make a request about patient or caller information

If you are a patient or caller and want to see, get a copy of, correct or delete information about you, ask how it was used or disclosed, or make any other request about your health information, **please contact your dental practice directly**. The Practice is responsible for responding to your request, and it can use the dashboard to find, export and delete call records.

If you send a request about Practice Data to us, we will forward it to the relevant Practice where we can identify it, and help the Practice respond as our agreements with it and the law require. We will not respond to the substance of the request ourselves except as the Practice directs or the law requires. To help us route your request, please tell us the name of the dental practice you called, its location, and the approximate date of the call.

2.3 What callers should know

- **You are talking with an AI system.** The AI receptionist is an AI system, not a person. It can make mistakes, such as mishearing a name or a date. If something matters, confirm it with the Practice's staff.
- **Emergencies.** The AI receptionist does not give medical, dental or emergency advice and Palmyra is not an emergency service. If you have a life-threatening emergency, hang up and dial 911.
- **Recording.** Call recording is off unless a Practice turns it on, and then a disclosure plays at the start of the call. Calls are transcribed and summarized either way so the Practice can follow up.
- **Practice integrations.** If the Practice has connected its practice management system through NexHealth, or a calendar, appointment details are exchanged with it on the Practice's instructions. NexHealth may send you its own appointment confirmation.
- **Retention.** Call records are deleted automatically after the Practice's plan history window (Section 8).

3. Personal information we collect

This section covers website visitors, prospects and Practice users. The table in Section 3.4 summarizes categories, sources, purposes and recipients.

3.1 Information you give us

- **Contact data**, such as your name, work email address, phone number, job title and Practice name. Our early-access form asks only for your email address.
- **Account data:** your name, email address, role (owner, admin or member) and password. We store passwords only as a one-way hash (bcrypt). If you turn on multi-factor authentication, we store your authenticator secret encrypted and your recovery codes as hashes.
- **Practice setup data**, such as the Practice's locations, hours, providers, front-desk number, time zone, FAQs and insurance accepted. This is mostly business information but may include staff names and work contact details.

- **Agreement records.** When you accept our Terms of Service or sign our Business Associate Agreement, we record your typed name, the version, the date and time, your IP address and your browser's user agent.
- **Billing data,** such as the billing contact's name, email and address, and plan and subscription history. Payment card details are entered on pages hosted by Stripe and are collected and held by Stripe, never by Palmyra.
- **Communications data,** such as support requests and other messages you send us, and our replies.

3.2 Information collected automatically

- **Security and session data:** your sign-up IP address (kept to prevent fraud and abuse), the IP address and user agent of each session (up to 7 days), your last sign-in time and whether you have verified your email address.
- **Audit-log data.** To meet our HIPAA obligations, we keep a tamper-evident log of dashboard actions, including access to Practice Data and administrative changes, with the user, time, IP address and user agent.
- **Performance and error data.** The dashboard uses Amazon CloudWatch RUM to collect page-load timing, JavaScript errors and browser and device type. It does not use cookies or capture the contents of your requests.
- **Server logs,** such as IP address, time, the address requested and error details.
- **Third-party website resources.** Our website loads fonts from Google Fonts and icons from the unpkg content delivery network, so those providers receive your IP address and browser information.

We do not collect precise geolocation, and we do not use advertising identifiers, email tracking pixels, or third-party analytics or advertising tags. See Section 6 and our Cookie Notice (<https://palmyra.life/cookies>).

3.3 Information from other sources

- **Your Practice,** when an owner or administrator invites you to the dashboard (your name, email and role).
- **Service providers,** such as payment status from Stripe, email delivery status from Resend, and the result of the Cloudflare Turnstile check at sign-up.
- **Business contacts,** such as a colleague who refers you to us.

3.4 Summary table

Category	Examples	Sources	Main purposes	Disclosed to
Identifiers and contact data	Name, work email, phone number, job title, Practice name, IP address	You; your Practice; your device	Provide and support the Service, communicate with you, security	Hosting and email providers; payment processor (billing contacts)
Account login credentials	Email and password (stored as a hash), MFA secret (encrypted), recovery codes (hashed)	You	Authenticate you and secure your account	Hosting provider only
Commercial and billing information	Plan, subscription, invoices, usage, billing contact	You; Stripe	Billing, account administration, fraud prevention	Stripe; hosting provider
Internet and device activity	Session IP and user agent, sign-in times, audit-log entries, error and performance data, server logs	Your device; the Service	Security, HIPAA audit trail, troubleshooting, improving the Service	AWS (hosting, monitoring); Cloudflare (sign-up check)
Professional information	Role in the Practice, Practice setup data	You; your Practice	Provide the Service	Hosting provider
Records of agreements	Typed name, version, timestamp, IP, user agent for Terms and BAA acceptance	You; your device	Show contract acceptance, legal compliance	Hosting provider; professional advisors if needed
Communications	Support emails, feedback, early-access email address	You	Respond to you, support, product updates	Email and hosting providers

In the terms used by the California Consumer Privacy Act, the categories above are identifiers, customer records (Cal. Civ. Code §1798.80), commercial information, internet or other electronic network activity information, and professional or employment-related information. Account login credentials are "sensitive personal information" under that law. Practice Data is not included in this table because we process it on the Practice's behalf (see Section 2), and protected health information is generally exempt from state consumer privacy laws.

4. How we use personal information

We use the personal information described in Section 3 for the following purposes, or as otherwise described when we collect it.

- **To provide and operate the Service:** create and maintain accounts and team memberships; authenticate users and secure sessions; set up a Practice's AI receptionist, phone numbers and settings; process subscriptions, usage charges and invoices through Stripe; send service emails such as verification, invitations, security alerts, billing notices and the call and message notifications a Practice chooses; record acceptance of our agreements; and respond to support requests.
- **To communicate with prospects** about early access and information about Palmyra you asked for. You can opt out at any time (Section 10).
- **To keep the Service secure:** detect, prevent and investigate fraud, abuse, spam sign-ups and security incidents, enforce rate limits, and keep the audit log HIPAA requires.
- **To maintain and improve the Service:** troubleshoot errors, monitor performance and reliability, understand how features are used, and develop new features, using account, usage and technical information and de-identified or aggregated data.
- **To comply with law and protect rights:** comply with laws and legal process, meet our HIPAA and contractual obligations, audit our compliance, enforce our Terms of Service, and protect the rights, privacy, safety or property of Palmyra, our customers, callers or others, including by making or defending legal claims.
- **For business transactions,** as described in Section 5.
- **With your consent or at your direction,** for any other purpose we describe to you at the time.

De-identified and aggregated data. We may create information that does not identify any individual or Practice, such as total call volumes across the Service, and use it to operate, analyze and improve the Service. We will not try to re-identify it (except as the law permits to test our methods), and we require anyone who receives it to agree to the same. We de-identify protected health information only as our Business Associate Agreement and HIPAA allow. We do not use protected health information to train AI models.

We do not use personal information for targeted advertising, and we do not use it to make decisions based solely on automated processing that produce legal or similarly significant effects about you.

5. How we disclose personal information

We disclose personal information only as described in this Privacy Policy, as described when we collect it, or with your consent.

Service providers. We use service providers to host and operate the Service on our behalf. They may use personal information only to provide services to us, under contracts that restrict their use of it. Our main service providers are Amazon Web Services (hosting, database, file storage, encryption keys, logging and monitoring, in the United States), Twilio (phone numbers and call connectivity), LiveKit (real-time voice infrastructure), OpenAI (the AI model that powers the AI receptionist's conversations and call summaries), Stripe (payments and billing), Resend (transactional email) and Cloudflare (bot protection at sign-up). The current list of our subprocessors, and what each one does, is at <https://palmyra.life/subprocessors>.

Payment processor. Stripe collects and processes payment card details directly when you subscribe or manage billing. Stripe uses that information under its own privacy policy, available at <https://stripe.com/privacy>.

Your Practice. Your name, email, role and dashboard activity are visible to your Practice's owners and administrators, and your name to other members of its team.

Integrations a Practice chooses. If a Practice connects a service such as NexHealth or Google Calendar, we exchange information with it on the Practice's instructions, under the Practice's own agreement with that service.

Professional advisors, such as lawyers, accountants, auditors and insurers, under duties of confidentiality.

Legal requirements and protection. We may disclose information to law enforcement, government authorities, courts or others if we believe in good faith that the law requires it (for example, a subpoena or court order) or that it is necessary to protect the rights, privacy, safety or property of Palmyra, our customers, callers or others. For Practice Data, we make such disclosures only as our Business Associate Agreement and HIPAA allow and, where the law permits, we will tell the Practice about the request.

Business transfers. We may disclose information to actual or prospective investors, lenders, buyers and their advisors in connection with a financing, merger, acquisition, sale of all or part of our business or assets, or insolvency, bankruptcy or receivership, and information may transfer to a successor. Recipients must protect it consistently with this Privacy Policy, and Practice Data remains subject to our Business Associate Agreement.

De-identified and aggregated information, as described in Section 4.

We do not disclose personal information to data brokers or advertising partners.

6. Cookies and similar technologies

Our full Cookie Notice is at <https://palmyra.life/cookies>. In summary:

- **Website (<https://palmyra.life>).** Our website does not set cookies and does not use analytics, advertising or social-media tracking technologies. When the page loads fonts from Google Fonts and icons from unpkg, those providers receive your IP address and browser information.
- **Dashboard (<https://app.palmyra.life>).** The dashboard uses two strictly necessary cookies to keep you signed in securely: `access_token`, which lasts 15 minutes, and `refresh_token`, which lasts 7 days. Both are `httpOnly`, `Secure` and `SameSite=Strict`. The dashboard also uses your browser's local storage and session storage for convenience settings, such as the phone number you last selected, a draft of your onboarding answers (such as Practice name, front-desk number and time zone), navigation state, and whether you dismissed the setup guide.

- **Monitoring and bot protection.** The dashboard uses Amazon CloudWatch RUM, without cookies, for error and performance data. Our sign-up page may show a Cloudflare Turnstile challenge, which processes browser and device information to stop automated sign-ups.
- **Payment pages** are hosted by Stripe, which sets its own cookies under its own privacy policy.

Because we use only strictly necessary technologies, we do not show a cookie consent banner. You can block or delete cookies in your browser settings, but the dashboard will not work without its sign-in cookies.

Do Not Track and Global Privacy Control. Some browsers send "Do Not Track" or Global Privacy Control signals. Because we do not sell personal information, share it for cross-context behavioral advertising, or engage in targeted advertising, there is no such activity for those signals to stop. Where the law requires, we treat a Global Privacy Control signal as a valid request to opt out of sale and sharing.

7. We do not sell or "share" personal information

Palmyra does not sell personal information, and has not sold personal information in the past 12 months. We do not "share" personal information for cross-context behavioral advertising, as that term is used in California law, and we do not process personal information for targeted advertising, as that term is used in other state privacy laws. We do not sell sensitive personal information, and we do not use or disclose sensitive personal information to infer characteristics about anyone. We do not have actual knowledge that we sell or share personal information of anyone under 16 years of age.

If we ever change these practices, we will update this Privacy Policy first and give you any notice and choice the law requires.

8. How long we keep personal information

We keep personal information only as long as we need it for the purposes in this Privacy Policy, including meeting legal and contractual obligations and resolving disputes, and then delete or de-identify it.

Information	How long we keep it
Call records, transcripts, summaries, recordings, voicemails, messages, callback, refill and intake requests (Practice Data)	For the call-history window of the Practice's plan (30 days on Starter, 90 days on Pro, or as agreed for Enterprise), then deleted automatically, including stored files. Recording files also have a backstop deletion after about 400 days.
Other Practice Data and account data, after a Practice closes its account	Service stops immediately at closure; remaining data is permanently deleted 30 days later. Practices can export their data from the dashboard before closing.
Dashboard session records (IP address and user agent)	Up to 7 days

Information	How long we keep it
Audit-log entries, including records of access to Practice Data and administrative actions	6 years, in write-once storage, as HIPAA documentation rules require
Records of Terms and BAA acceptance, billing and tax records	While the account is open, then as long as needed for legal, tax and accounting requirements and legal claims
Database backups	Roll off after 7 days
Operational and server logs	Up to 1 year
Early-access and prospect contact details	Until you ask us to remove them or we no longer need them to contact you about Palmyra
Support communications	While the account is open, then as needed for disputes and legal obligations

A Practice can also delete call records sooner, and our Business Associate Agreement governs what happens to Practice Data when our agreement with a Practice ends.

9. Security

We use administrative, technical and physical safeguards designed to protect personal information, including:

- encryption of data in transit using TLS;
- application-level encryption (AES-256-GCM envelope encryption, with support for key rotation) of sensitive text, including transcripts, summaries, messages, intake answers, refill notes, practice management system credentials and multi-factor authentication secrets;
- encryption of stored recordings and files, with public access blocked, and encrypted database storage;
- separation of each Practice's data, enforced in our application;
- role-based access, with sensitive actions limited to a Practice's owners and administrators;
- optional multi-factor authentication, email verification, rate limiting and sign-up abuse controls;
- a tamper-evident, hash-chained audit log of access to protected health information and administrative actions, archived to write-once storage for 6 years; and
- infrastructure activity logging (AWS CloudTrail) and automated alerts.

No method of transmission or storage is completely secure, and we cannot guarantee the security of personal information. You are responsible for keeping your password and authenticator device safe, and we encourage every Practice user to turn on multi-factor authentication. If we become aware of a security incident affecting personal information, we will notify affected Practices and individuals as required by law and by our agreements, including our Business Associate Agreement. To report a security concern, email privacy@palmyra.life.

10. Your choices

- **Account and security.** You can review certain account details, turn on multi-factor authentication and manage your active sessions in the dashboard. A Practice's owners and administrators can change your role or remove your access.
- **Export and closure.** A Practice's owner can export the Practice's data and close the account from the dashboard (see Section 8).
- **Emails.** You can unsubscribe from early-access and other information about Palmyra using the link in the email or by contacting privacy@palmyra.life. Practice users will still receive emails needed to provide the Service, such as security, verification and billing notices.
- **Cookies.** See Section 6 and our Cookie Notice.
- **Declining to provide information.** If you do not provide information we identify as required, such as an email address for an account, we may not be able to provide the Service.

11. US state privacy rights

11.1 Who this section applies to

Several US states, including California (under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, "**CCPA**"), Texas (under the Texas Data Privacy and Security Act, "**TDPSA**"), and others such as Colorado, Connecticut, Oregon and Virginia, give their residents rights over their personal information (together, "**State Privacy Laws**"). This section applies to residents of those states to the extent a State Privacy Law applies to us and to the information involved. In this section, "personal information" and "sensitive personal information" have the meanings those laws give them (including "personal data" and "sensitive data").

Please keep in mind:

- **Most information we hold is business-to-business.** Several State Privacy Laws, including the TDPSA, do not cover people acting in a commercial or employment context, such as Practice staff using the dashboard for work. California's law does.
- **Patient and caller information is handled for the Practice.** Protected health information is generally exempt from State Privacy Laws, and some of those laws exempt HIPAA business associates entirely. For information we process for a Practice, the Practice responds to requests (see Section 2.2).
- **Rights are not absolute.** We may decline or limit a request where the law allows, for example if we cannot verify your identity or need the information for security or to meet a legal obligation, and we will explain why.

Where a State Privacy Law does not strictly apply, we will still consider requests from Practice users and prospects in good faith.

11.2 Your rights

Depending on your state of residence, you may have the right to:

- **Know and access.** Confirm whether we process your personal information and get a copy, in a portable format where required. California residents may also ask for the categories of personal information, sources, purposes and recipients for the prior 12 months.
- **Delete.** Ask us to delete personal information we have collected from or about you.
- **Correct.** Ask us to correct inaccurate personal information about you.
- **Opt out.** Opt out of the sale of personal information, its "sharing" for cross-context behavioral advertising, its processing for targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects. We do not do any of these things (see Sections 4 and 7), but you may still submit an opt-out request and we will record it.
- **Limit use of sensitive personal information.** We use sensitive personal information (your account login credentials) only to provide and secure the Service, as the CCPA permits, and not to infer characteristics about you, so the right to limit does not apply.
- **Appeal.** Appeal our decision on your request (see Section 11.4).
- **Non-discrimination.** We will not deny you the Service, charge a different price or provide a different quality because you exercised a privacy right.

11.3 How to make a request

To exercise these rights, email privacy@palmyra.life with the subject line "Privacy Request", or write to us at [COMPANY MAILING ADDRESS]. Please tell us which right you want to exercise, your state of residence, and how you relate to Palmyra (for example, website visitor, early-access contact, or user at a named Practice). If you are a Practice user, sending the request from the email address associated with your account helps us verify it.

Verification. Before acting on a request to access, delete or correct information, we will verify your identity by matching information you give us with information we hold, for example by asking you to confirm control of the email address on file or to sign in. We use information provided for verification only for that purpose. Opt-out requests do not need verification, but we may decline one we reasonably believe is fraudulent.

Authorized agents. Where the law allows, you may use an authorized agent. Unless the agent holds a valid power of attorney, we may ask for proof of your signed permission and ask you to verify your identity or confirm the request directly.

Timing and fees. We will confirm receipt within 10 business days where the CCPA requires and respond within 45 days, which we may extend by up to 45 more days where the law allows, telling you why. We do not charge a fee unless a request is manifestly unfounded, excessive or repetitive, as the law allows.

11.4 Appeals

If we decline your request in whole or in part, you may appeal within a reasonable time by replying to our decision or emailing privacy@palmyra.life with the subject line "Privacy Request Appeal". We will respond in writing, with our reasons, within the period your state's law requires (60 days for Texas residents; 45 days in most other states that provide this right). If we deny your appeal, you may contact the attorney general of your state. Texas residents may submit a complaint to the Texas Attorney General at www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint.

11.5 Our practices in the past 12 months

In the 12 months before the effective date of this Privacy Policy, we collected the categories of personal information in Section 3 from the sources and for the purposes in Sections 3 and 4, disclosed them for business purposes to the recipients in Section 5, and kept them as described in Section 8. We did not sell or share personal information or process it for targeted advertising, and the only sensitive personal information we collected was account login credentials, used only to provide and secure the Service.

Other state notices. We do not disclose personal information to third parties for their own direct marketing (California "Shine the Light", Cal. Civ. Code §1798.83). We do not sell covered information under Nevada law. We do not sell sensitive personal data or biometric data as defined by the TDPSA.

12. Children

Our website and dashboard are designed for dental practices and their staff and are not directed to children. We do not knowingly collect personal information through them from children under 13, or knowingly allow anyone under 16 to create a dashboard account. If you believe a child under 13 has given us personal information, contact privacy@palmyra.life and we will delete it as the law requires.

The AI receptionist may process information about a child who is a patient when a parent, guardian or the child calls a Practice. That is Practice Data, handled as described in Section 2; requests about it should go to the Practice.

13. Other websites and services

The Service may link to, or work with, websites and services that we do not operate, such as Stripe's payment pages, NexHealth, Google Calendar and the websites of our service providers. We are not responsible for the privacy practices of those services, and this Privacy Policy does not apply to them. Please read their privacy policies.

14. Where we process information

Palmyra is based in, and offers the Service only in, the United States. We store Service data with Amazon Web Services in the United States (us-east-1 region), and our service providers process it in the United States.

15. Changes to this Privacy Policy

When we update this Privacy Policy, we will post the new version here and change the effective date. For material changes, we will also notify Practice account owners by email or through the dashboard before the change takes effect, where practicable. If the law requires your consent to a change, we will ask for it. Changes do not reduce our obligations to Practices under our Business Associate Agreement or other agreements, which can be changed only as those agreements provide.

16. How to contact us

If you have questions about this Privacy Policy or our privacy practices, or want to exercise a privacy right, contact us at:

- **Email:** privacy@palmyra.life
- **Mail:** [PALMYRA LEGAL ENTITY NAME], Attn: Privacy, [COMPANY MAILING ADDRESS]

To report a security concern, email privacy@palmyra.life. For help with your account, email support@palmyra.life.

If you are a patient or caller with a question about your health information, please contact your dental practice first (see Section 2.2).

Adapted from a template prepared by General Legal, PC and released under CCo 1.0. General Legal has not reviewed this adaptation, and it is not legal advice.