

DDSALLY LLC

Privacy Policy

For dental practices, dentists, providers, specialists, and authorized dental office staff

Effective Date	6/2/2026
Last Updated	6/2/2026
Website	https://ddsally.com
Legal Contact	legal@ddsally.com
Privacy Contact	privacy@ddsally.com

This Privacy Policy explains how DDSALLY LLC ("DDSALLY," "we," "us," or "our") collects, uses, discloses, retains, and protects information when visitors, dental practices, dentists, providers, specialists, and authorized dental office staff use the DDSALLY website, platform, and related services (collectively, the "Service").

This Policy is designed for a clinician-to-clinician dental referral and secure communication platform. The Service is intended for dental professionals and authorized practice staff. It is not a patient portal and is not intended for direct use by patients or the general public.

1. Scope and Relationship to HIPAA

This Policy applies to Site visitors, practice administrators, dentists, dental providers, specialists, and staff members who create or use DDSALLY accounts. It describes DDSALLY's practices for non-patient account, usage, billing, support, and website information.

Patient information, including Protected Health Information ("PHI"), is handled differently. When DDSALLY processes PHI on behalf of a dental practice, DDSALLY acts as a Business Associate under HIPAA and processes that PHI according to the applicable Business Associate Agreement ("BAA"). Each dental practice remains responsible for its own patient Notice of Privacy Practices and patient-facing privacy obligations.

If this Policy conflicts with an executed BAA regarding PHI, the BAA controls for PHI.

2. Patient Communication Limitation

DDSALLY may allow a Practice or authorized provider to send secure messages, records, referral updates, instructions, or other patient-facing communications to a patient at the Practice's direction. In that situation, DDSALLY processes the information according to the BAA, the Practice's instructions, and applicable law.

DDSALLY does not allow patients to use the Service to send messages to offices, upload files, submit medical or dental information, provide histories, send images, request care, or otherwise communicate back to Practices through DDSALLY unless DDSALLY separately enables that functionality in writing and implements appropriate privacy, security, consent, and workflow controls.

If DDSALLY inadvertently receives patient-submitted medical, dental, clinical, imaging, diagnostic, or other PHI, DDSALLY may notify the relevant Practice and handle the information according to the BAA, HIPAA, and DDSALLY's applicable privacy and security procedures.

3. Information We Collect

- Account information: name, email address, phone number, login credentials, role, practice affiliation, and authentication settings.
- Practice information: practice name, address, NPI, specialty, license or credential information, administrator details, referral preferences, and onboarding information.
- Billing information: billing contact, billing address, subscription plan, transaction history, and payment metadata. Payment cards are processed by Stripe or another payment processor; DDSALLY does not store full card numbers on its servers. Payment processors should not receive PHI.
- Clinical and operational content: referral information, secure messages, patient-directed messages, attachments, images, DICOM files, PDFs, notes, and related content submitted through the Service by Practices or authorized Users. Some of this content may contain PHI and is governed by the BAA.
- Support and communications: information you provide when contacting support, security, privacy, or legal teams.
- Technical data: IP address, device identifiers, browser type, operating system, pages viewed, referring pages, timestamps, session data, and approximate location inferred from IP address.

DDSALLY LLC

- Usage data: login events, feature usage, workflow actions, settings changes, referral status actions, patient-directed send events, and other interactions with the Service.
- Security and audit logs: authentication events, access attempts, content access, downloads, administrative changes, user invitations, message transmission events, and other events needed for security monitoring and HIPAA audit support.
- Cookies and similar technologies: session cookies, preference cookies, and analytics or performance technologies as described below.
- Third-party information: public or professional registries when used to verify licensing or professional eligibility; payment processors for transaction status and billing metadata; and service providers that help us operate, secure, or support the Service.

4. How We Use Information

- Provide, operate, maintain, secure, and improve the Service.
- Create and administer accounts for practices, dentists, providers, specialists, and authorized staff.
- Authenticate users, enforce multi-factor authentication, and secure accounts.
- Process subscriptions, billing, invoices, and payment-related communications.
- Enable referral coordination, secure file exchange, clinical messaging, Practice-to-patient message delivery, workflow management, and audit logging.
- Send transactional communications such as verification codes, password resets, security alerts, billing notices, service announcements, and support responses.
- Detect, prevent, investigate, and respond to security incidents, fraud, abuse, unauthorized access, or policy violations.
- Comply with legal, regulatory, contractual, tax, accounting, and HIPAA-related obligations.
- Analyze usage trends, improve performance, develop features, and create aggregated, anonymized, or de-identified information for internal analytics and product improvement.
- Send marketing or product updates where permitted by law and subject to opt-out rights.

5. How We Share Information

With authorized practices and users, the Service is collaborative. Referral content, messages, patient-directed communications, and attachments may be visible to authorized users at the sending practice, receiving practice, and other authorized practices selected within the referral workflow. Practice administrators may view user activity and audit information associated with their practice account.

With patients at a Practice's direction: DDSALLY may transmit secure messages or information to a patient only when directed by a Practice or authorized provider. DDSALLY is not responsible for incorrect patient contact information, wrong recipient selection, inaccurate PHI submitted by the Practice, or misuse of patient-directed messaging by a Practice or its Users.

With service providers and subprocessors: DDSALLY may share information with service providers and subprocessors that help host, secure, support, analyze, bill for, or operate the Service. Where a subprocessor handles PHI, DDSALLY will require appropriate contractual protections, including a BAA where required.

DDSALLY may maintain a current list of subprocessors that handle PHI or support the Service, and may make that list available through the Service, on a designated webpage, during onboarding, or upon reasonable request to privacy@ddsally.com.

AWS or similar cloud infrastructure may be used for hosting, storage, databases, logging, encryption, identity, email delivery, and related infrastructure. PHI should be processed only in HIPAA-eligible services under DDSALLY's applicable BAA and configured HIPAA controls.

Stripe or another payment processor may process payment and billing information. Payment processors should not receive PHI.

Error monitoring, analytics, and performance tools should be configured to avoid, scrub, aggregate, de-identify, or otherwise protect PHI as appropriate.

DDSALLY may disclose information when reasonably necessary to comply with law, regulation, legal process, or governmental request; protect the rights, safety, or property of DDSALLY, practices, users, patients, or others; detect or prevent fraud, abuse, or security incidents; or enforce our Terms of Service or other agreements.

If DDSALLY is involved in a merger, acquisition, financing, reorganization, bankruptcy, or sale of assets, information may be transferred as part of that transaction, subject to applicable law, BAA obligations, and confidentiality protections.

DDSALLY does not sell personal information as "sale" is commonly defined under the CCPA/CPRA, does not share personal information for cross-context behavioral advertising, and does not sell PHI.

DDSALLY LLC

6. HIPAA and Patient Information

DDSALLY may receive, create, maintain, transmit, or store PHI for dental practices. In that role, DDSALLY is a Business Associate, and the dental practice is generally the Covered Entity. DDSALLY will use and disclose PHI only as permitted by the applicable BAA, HIPAA, and the Practice's instructions through the Service.

Dental practices are responsible for ensuring they have the legal right to submit patient information to the Service and to send patient-facing communications through the Service, including any patient authorization, consent, or acknowledgment required by HIPAA, state privacy laws, dental practice laws, or professional obligations.

Patients who have privacy-rights requests involving PHI should generally contact the dental practice that provided or received the patient's information. DDSALLY may direct patient requests to the relevant Practice unless DDSALLY is required by law to respond directly.

7. Data Retention

- DDSALLY retains information for as long as necessary to provide the Service, maintain accounts, comply with legal obligations, resolve disputes, enforce agreements, and support security, audit, and clinical record obligations.
- Clinical referral content, patient-directed messages, and related communications may be retained as part of the sending or receiving Practice's clinical, referral, or designated record set for the longer of HIPAA retention requirements, applicable state dental record retention laws, payer or professional requirements, and special rules for minors.
- Audit logs are retained for at least six years or longer if required by law, contract, security needs, or HIPAA-related obligations.
- Billing and accounting records are retained as required by tax, accounting, and business laws.
- Closed-account personal identifiers may be deleted, anonymized, or limited upon request where legally permissible, but deletion will not compromise required clinical records, audit logs, security evidence, backup systems, or records retained on behalf of another Practice.

8. Security

DDSALLY implements administrative, technical, and physical safeguards designed to protect information, including safeguards aligned with the HIPAA Security Rule. These may include encryption in transit and at rest, role-based access controls, unique user accounts, multi-factor authentication, audit logs, vulnerability management, backup and recovery controls, least-privilege access, vendor risk management, and incident response procedures.

No system can be guaranteed completely secure. Users must maintain strong passwords, protect credentials, use MFA, promptly remove access for departing staff, verify recipient information before sending PHI, and notify DDSALLY immediately of suspected unauthorized access at security@ddsally.com.

9. Cookies and Tracking Technologies

DDSALLY may use cookies, local storage, and similar technologies to maintain authenticated sessions, remember preferences, improve performance, detect fraud, secure the Service, and understand usage. Essential cookies are required for the Service to function. Non-essential analytics or marketing cookies, if used, will be implemented in accordance with applicable law and consent requirements.

You can control cookies through your browser settings. Disabling essential cookies may prevent the Service from working properly. DDSALLY honors legally required opt-out preference signals such as Global Privacy Control where applicable.

10. Your Privacy Rights

Depending on your jurisdiction, you may have rights to access, correct, delete, restrict, object to, or receive a portable copy of certain personal information. California residents may have additional rights under the CCPA/CPRA, including the right to know categories of information collected, used, disclosed, and retained.

To exercise rights, contact privacy@ddsally.com from the email associated with your account. DDSALLY may need to verify your identity and authority before fulfilling a request. Requests involving PHI may need to be directed to the relevant dental practice, because the practice is responsible for patient rights under HIPAA.

11. International Users

DDSALLY is designed for use in the United States and stores information in the United States unless otherwise stated. If you access the Service from outside the United States, you understand that information may be transferred to and processed in the United States, where privacy laws may differ from those in your jurisdiction.

DDSALLY LLC

12. Children's Privacy

The Service is not intended for use by children or by anyone under 18. DDSALLY does not knowingly collect personal information directly from children through account registration. Patient information about minors may be processed only when submitted by authorized dental professionals and governed by the applicable BAA and practice obligations.

13. Changes to This Policy

DDSALLY may update this Policy from time to time. Material changes will be posted on the Site or communicated to practice administrators or users by email or in-product notice where required. Continued use of the Service after the effective date of a revised Policy means the revised Policy applies going forward.

14. Contact

- Privacy Officer: privacy@ddsally.com
- Security: security@ddsally.com
- Support: support@ddsally.com
- Legal: legal@ddsally.com
- Mailing Address: 5757 Wilshire Blvd., PR5, Los Angeles, CA 90036, USA