CliniShot

Privacy Policy

Document version	2.0
Effective date	May 7, 2026
Last updated	May 7, 2026
Public URL	https://clinishot.com/privacy
Applicable law	Brazilian LGPD (Federal Law No. 13,709/2018)
Languages available	English

1. Introduction

This Privacy Policy explains how CliniShot collects, uses, shares, retains, and protects personal data when you use the CliniShot mobile application (iOS and Android), web application, and related services (collectively, the "Service"). It is written to comply with the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados – LGPD, Federal Law No. 13,709/2018), and to be transparent and consistent with the disclosures that CliniShot provides to the Apple App Store and the Google Play Store.

By creating an account or using the Service, you confirm that you have read and understood this Policy. If you do not agree with any part of it, you must not use the Service. CliniShot is operated by Levius Consultoria Empresarial Ltda., a company registered in Brazil under CNPJ 22.665.714/0001-51, with registered office at Rua Barão de Saquarema, 379, Sala 03 Parte, Centro, Saquarema, RJ, CEP 28990-772, Brazil, hereinafter referred to as "CliniShot", "we", "us", or "our".

2. Data Controller and Data Protection Officer

CliniShot acts as the controller of personal data of its direct users (healthcare professionals, clinics, and account administrators) within the meaning of LGPD Art. 5(VI). With respect to clinical data and images of patients uploaded by healthcare professionals, CliniShot acts as an operator (Art. 5(VII)) on behalf of the healthcare professional or clinic, who remains the controller of patient data. When patients themselves are granted access to the Service to receive reports or images, CliniShot acts as a controller of the limited personal data of that patient relationship (account access, authentication, communications) and as an operator of the underlying clinical content.

Contact for privacy matters

- Data Protection Officer: Gustavo Alexandre Monteiro da Silva
- General privacy inquiries: support@clinishot.com

- Postal address: Rua Barão de Saquarema, 379, Sala 03 Parte, Centro, Saquarema, RJ, CEP 28990-772, Brazil

You also have the right to lodge a complaint with the Brazilian National Data Protection Authority (ANPD) at www.gov.br/anpd. We encourage you to contact us first so we can address your concern directly.

3. Scope and Categories of Users

CliniShot is designed for use by adults (18 years of age or older) in their professional or institutional capacity. The Service distinguishes between three categories of users:

- **Healthcare professionals and clinics** — licensed practitioners and institutions that create accounts to manage clinical photographs and records of their patients.
- **Account administrators** — individuals authorized by a clinic to manage user access, billing, and configurations.
- **Patients** — in features where a healthcare professional shares content directly with their patient through the Service.

The Service is not directed to, and is not intended for, the general public, the unsupervised use by patients, or use as a self-diagnosis tool.

4. Data We Collect

We only collect personal data that is necessary for the purposes of our service.

Category	Examples of data	Purpose	Legal basis (LGPD)
Identification & Contact	Full name, professional registration (CRM/CRO/COREN/CRP/etc.), email address, phone number, professional affiliation	Account creation, authentication, communication, regulatory compliance	Contractual necessity (LGPD Art. 7, V) and Legal obligation
Authentication & Account	Username, hashed password, multi-factor authentication tokens, session tokens, account preferences	Authentication, account security, session management	Contractual necessity
Health & Clinical Data (uploaded by professional)	Patient clinical photographs, anatomical images, clinical notes, procedure annotations, treatment metadata	Clinical documentation, follow-up, sharing with the patient or other authorized professionals at the user's discretion	Operator on behalf of healthcare professional; sensitive data processed under LGPD Art. 11 with the basis the professional has obtained from the patient

Category	Examples of data	Purpose	Legal basis (LGPD)
Camera & Photo Library Content	Photographs captured in-app or imported from the device's photo library by the professional	Capturing and importing clinical images	Contractual necessity (the user actively initiates each capture/import)
Usage & Diagnostic Data	Device type, operating system and version, app version, IP address, access timestamps, feature usage logs, crash reports	Security, fraud prevention, debugging, performance monitoring, service improvement	Legitimate interest (LGPD Art. 7, IX) with balancing test
Cookies & Web Identifiers (web app only)	Session cookies, authentication cookies, strictly-necessary functional cookies	Maintaining your login and preferences	Legitimate interest for strictly-necessary cookies; consent for any non-essential cookies
Support Communications	Support tickets, email correspondence, in-app chat content with our support team	Providing user support and resolving issues	Contractual necessity
Billing Data (paid plans)	Subscription tier, billing contact, invoice history. Card data is processed directly by our payment processor and is not stored by CliniShot.	Processing payments and complying with tax obligations	Contractual necessity and Legal obligation

5. Permissions We Request on Your Device

The Service requests only the permissions necessary to deliver its core functionality. Each permission corresponds to an iOS purpose string (NS*UsageDescription) or an Android runtime permission and is requested only at the moment the user invokes the related feature.

Permission	Platform key	Why we need it
Camera	iOS: NSCameraUsageDescription • Android: CAMERA	Required to capture clinical photographs in-app. Only invoked when the user taps the in-app camera control.
Photo Library	iOS: NSPhotoLibraryUsageDescription / NSPhotoLibraryAddUsageDescription • Android: READ_MEDIA_IMAGES	Required to import existing clinical images from the device, and to optionally export images back to the gallery.

Permission	Platform key	Why we need it
Push Notifications	iOS: User Notifications framework • Android: POST_NOTIFICATIONS	Used to notify the user about sharing events, account security alerts, and account updates. Optional; the Service works without notifications.
Network access	Implicit on iOS • Android: INTERNET	Required to synchronize data with the CliniShot servers and to deliver the Service.
Face ID / Biometric authentication	iOS: NSFaceIDUsageDescription • Android: USE_BIOMETRIC	Optional. Used only locally on the device to unlock the app. CliniShot never receives or stores biometric templates; authentication is performed by the device's secure enclave. CliniShot does not use facial recognition or biometric identification technology. Clinical photographs, including those that may contain patients' faces, are stored solely as medical records for clinical documentation purposes. These images are not analyzed to identify, map, or verify the identity of individuals.

You may revoke any of these permissions at any time in your device's system settings. Revoking a permission may disable the related feature.

6. How We Use Your Data

We process personal data only for the purposes disclosed in this Policy and only on the legal bases listed in Section 4 and Section 7.

- **Service delivery —** operating the core features (image capture, organization, storage, sharing, export) and synchronizing data across your devices.
- **Account management and security —** creating and authenticating accounts, preventing unauthorized access, detecting fraud and abuse.
- **Support and service communications —** responding to inquiries, sending transactional notifications (e.g., security alerts, billing, policy changes).
- **Service improvement —** diagnosing issues, monitoring performance, and refining features. Whenever feasible, this is performed on aggregated or de-identified data.
- **Legal compliance —** complying with LGPD, healthcare-related regulations, tax law, judicial orders and lawful requests by competent authorities.

We do not use personal data for behavioral advertising and we do not sell personal data.

7. Legal Bases for Processing

Under LGPD, we rely on the following legal bases:

- **Execution of contract (Art. 7, V)** — for delivering the Service to the user who signed up.
- **Compliance with legal or regulatory obligation (Art. 7, II)** — for tax, accounting and judicial requirements.
- **Legitimate interest (Art. 7, IX)** — for security, fraud prevention, debugging, and service improvement, balanced against your rights and freedoms. A balancing test is documented and available upon request.
- **Consent (Art. 7, I)** — for processing activities that are not strictly necessary, such as use of optional third-party AI features (Section 9) and use of de-identified data for AI model training (Section 9.4).
- **Protection of life and health (Art. 7, IV; Art. 11, II, "f")** — when strictly applicable in exceptional clinical urgency contexts.

For sensitive personal data (including health data), we additionally apply the conditions of LGPD Art. 11, principally relying on the consent obtained by the healthcare professional from the patient, and on our role as operator on the professional's behalf.

8. Third-Party Service Providers

We use the following sub-processors and service providers to operate CliniShot. Each is bound by contract to process personal data only on our instructions and to apply security measures consistent with this Policy. Before any provider is added or removed, this list will be updated and, where the change is material, we will notify users in advance.

Provider	Purpose	Hosting region	Data categories shared
CLOUD INFRASTRUCTURE, Amazon Web Services	Cloud hosting, storage, compute, backups	Data is primarily stored in Brazil (region sa-east-1 of Amazon AWS)	All data categories at rest
DATABASE — Supabase / Managed PostgreSQL	Database, authentication, row-level security	Data is primarily stored in Brazil (region sa-east-1 of Amazon AWS)	All structured data
OBJECT STORAGE — AWS S3 / Supabase Storage	Storage of clinical images and exports	Data is primarily stored in Brazil (region sa-east-1 of Amazon AWS)	Health & clinical data, photos
EMAIL DELIVERY — SendGrid, Resend	Transactional email (verification, alerts)	Global Infrastructure	Identification & contact
PAYMENT PROCESSOR — Stripe, Revenue Cat	Subscription billing and payments	Global Infrastructure	Billing data (card data is held only by the processor; CliniShot does not store card numbers)
ERROR / CRASH REPORTING — Sentry	Crash and error monitoring	Global Infrastructure	Diagnostics, device identifiers (no personal content of clinical records)
AI PROVIDER — Anthropic, OpenAI,	Processing of images or text for the specific AI	Global Infrastructure	Only the data submitted to the AI feature in that operation; see Section 9

Provider	Purpose	Hosting region	Data categories shared
Google Cloud, Pixian only when AI features are used	feature requested by the user		
PUSH NOTIFICATIONS — Firebase Cloud Messaging, OneSignal	Delivery of push notifications	Global Infrastructure	Device tokens and notification metadata only

9. Artificial Intelligence Features

9.1. Proprietary AI models

Some AI features run on models developed and hosted by CliniShot itself, within the same infrastructure described in Section 8. In that case, no personal data is sent to third-party AI providers.

9.2. Third-party AI components (opt-in, granular)

Certain optional features may rely on third-party AI providers, such as those listed in Section 8.

By signing in to the Service and accepting this Privacy Policy and the applicable Terms, the user expressly consents to the use of third-party AI providers for CliniShot AI features. However, no data is transmitted to a third-party AI provider merely by signing in. Data is transmitted only when the user chooses to invoke a specific AI feature, and only to the extent strictly necessary to provide that feature. By choosing to use a CliniShot AI feature, the user confirms their opt-in to the transmission and processing of the data necessary to provide that specific feature.

When you use a third-party AI feature:

• Only the data strictly necessary to deliver that feature is transmitted, typically the specific image or text submitted at that moment, plus minimal technical metadata.

• The data is processed by the AI provider solely for the purpose of returning the requested output.

9.3. AI assistance is not a clinical decision

Outputs from AI features are decision-support information, not clinical diagnoses. See the Medical Disclaimer in Section 16.

9.4. Use of de-identified data for AI training

CliniShot may use anonymized or de-identified clinical data to train, evaluate and improve proprietary AI models only where the data has undergone a documented anonymization or de-identification process and where the residual risk of re-identification is assessed as low. Where the data remains identifiable or reasonably re-identifiable, CliniShot will only use it for AI training with specific, prior, free and informed consent. For anonymized/de-identified datasets, users may opt out at any time by writing to support@clinishot.com. For identifiable or reasonably re-identifiable data, prior opt-in consent is required.

10. How We Share Your Data

Beyond the sub-processors listed in Section 8, we share personal data only in the following situations and only to the extent strictly necessary:

- **Sharing initiated by the user —** when a healthcare professional shares clinical content with another professional registered on CliniShot, or with their patient, through the Service's secure sharing features.
- **Healthcare institutions —** where the user is associated with a clinic or hospital account, account-level data and content created within that account may be visible to authorized administrators of that institution.
- **Legal and regulatory requirements —** judicial, ANPD, professional council, public health and tax authorities' lawful requests, in accordance with LGPD Art. 7, III.
- **Protection of rights and safety —** to investigate fraud, address security incidents, or defend our legal rights, our users' rights, or the public interest.
- **Corporate transactions —** in the event of merger, acquisition, reorganization or sale of the business, with the same level of protection guaranteed in this Policy. Users will be notified in advance of any such transfer.

We do not share personal data with third parties for their own marketing or advertising purposes, and we do not sell personal data.

10.1. International transfers

Data is primarily stored in Brazil (region sa-east-1 of Amazon AWS). Some sub-processors may store backups or replicate data to other regions. Whenever personal data is transferred outside Brazil, we rely on one of the legal mechanisms permitted by LGPD Art. 33, namely:

- Adequacy decision by the ANPD, when applicable; or
- Standard contractual clauses approved by the ANPD; or
- Specific consent of the data subject for the transfer, where required.

11. Data Security

We apply technical and organizational measures consistent with LGPD Art. 46–49, including:

- **Encryption in transit —** all communications between the apps, the web interface, and our servers use TLS 1.2 or higher with strong cipher suites.
- **Encryption at rest —** structured data and clinical images are encrypted at rest using AES-256 (or equivalent algorithm offered by the storage provider).
- **Access control —** role-based access, principle of least privilege, multi-factor authentication for administrative access, and detailed audit logs.
- **Network controls —** private subnets for databases, restricted security groups, web application firewall, and rate limiting.
- **Vulnerability management —** dependency scanning, periodic penetration tests, and a coordinated vulnerability disclosure channel at support@clinishot.com.
- **Operational practices —** background checks for staff with access to production data, signed confidentiality agreements, mandatory security and LGPD training, and secure software development practices.
- **Backup and recovery —** encrypted backups with documented retention and tested restore procedures.

No system is completely immune to security incidents. In the event of a personal data security incident that may pose relevant risk or harm to data subjects, we will notify the ANPD and the affected data subjects within a reasonable time, and in any event no later than 3 business days from the moment we become aware of the incident, in line with current ANPD guidance, providing the information required by LGPD Art. 48.

12. Data Retention

We retain personal data only as long as necessary to fulfill the purposes for which it was collected, or longer when required by law.

Data type	Retention period
Account data of healthcare professionals	While the account is active. Deleted within 30 days after account deletion request, except for data we must retain by law.
Clinical content (images, notes) on behalf of a professional	While the professional retains the content in the Service. Removed from active systems within 30 days after deletion request; backups are rotated and overwritten within 90 days.
Audit logs (security)	Retained for 12 months for security and incident response, or longer if required by a specific legal or regulatory obligation.
Billing and tax records	Retained for the period required by Brazilian tax and accounting legislation (typically 5 years from the relevant fiscal event).
Records of consent	Retained for the duration of the consent and for 5 years thereafter, to evidence compliance with LGPD.
Support tickets	Retained for 24 months after the ticket is closed.

13. Your Rights and How to Exercise Them

Under LGPD Art. 18, you have the right to:

- Confirm the existence of processing of your personal data.
- Access your personal data.
- Correct incomplete, inaccurate or outdated data.
- Anonymize, block or delete unnecessary, excessive or unlawfully processed data.
- Obtain data portability to another service provider, in a structured and interoperable format.
- Delete personal data processed on the basis of your consent.
- Be informed of public and private entities with which we shared your data.
- Be informed about the possibility of refusing consent and the consequences of doing so.
- Withdraw your consent at any time.
- Request the review of decisions taken solely based on automated processing that affects your interests, including AI-assisted decisions.

Requests may be submitted by email to support@clinishot.com. We may need to verify the requester's identity before fulfilling the request. Where CliniShot acts as an operator for patient clinical data, requests from patients may be redirected to the healthcare professional or clinic acting as controller, while CliniShot will provide reasonable assistance to such controller.

14. Children and Adolescents

CliniShot is intended exclusively for adults (18 years of age or older) acting in a professional or institutional capacity. Account creation is restricted to adults.

Patients under 18 may have personal data — including clinical photographs — uploaded to the Service by their healthcare professional. In this case:

- The healthcare professional, as controller of patient data, is responsible for obtaining the consent of the minor's parents or legal guardians, in accordance with LGPD Art. 14, and for ensuring that processing serves the minor's best interest.
- CliniShot, as operator, applies the same security and access-control measures as for adult patient data, and supports the controller in attending to data subject rights.
- If we become aware of the creation of an account by a minor in violation of these rules, we will deactivate the account and delete the associated personal data.

If you are a parent, legal guardian or any person who believes that data of a minor is being processed in a manner inconsistent with this Policy, please contact support@clinishot.com immediately.

15. Tracking and Advertising

CliniShot does not track users across apps and websites owned by other companies. CliniShot does not implement Apple's App Tracking Transparency framework because it does not perform the kinds of tracking that would require it. Specifically:

- We do not use the IDFA (Apple) or the Android Advertising ID (GAID) for tracking, profiling or advertising.
- We do not share device or user identifiers with data brokers or advertising networks.
- We do not display third-party advertising in the Service.

If this ever changes, we will (i) update this Policy in advance, (ii) implement the corresponding consent prompts (ATT on iOS, equivalent prompts on Android), and (iii) re-submit the Apple Privacy Nutrition Labels and Google Play Data Safety form accordingly.

16. Medical Disclaimer and Clinical Responsibility

CliniShot is a tool for clinical documentation and decision support. It is not a medical device certified by ANVISA, and it does not provide a medical diagnosis. The healthcare professional is solely responsible for clinical decisions made with or without the help of CliniShot, including diagnoses, treatment plans and communications with the patient.

AI-assisted suggestions, image analyses or summaries provided by CliniShot are informational outputs that the professional must independently review and validate before relying on them in clinical practice.

CliniShot is intended for clinical documentation, organization of images, and professional decision support. It is not intended to autonomously diagnose, prevent, monitor, treat or alleviate disease, nor to replace professional judgment.

17. Patient Consent and Healthcare Professional Obligations

When a healthcare professional uploads patient data to CliniShot, the professional acts as the controller of that data and is responsible for:

- Obtaining and documenting an appropriate legal basis under LGPD for the processing (typically the patient's free, informed, specific and documented consent for sensitive data, under Art. 11).
- Informing the patient about the use of CliniShot, including the categories of data uploaded, the purposes, the retention periods, and the patient's rights.
- Ensuring that any sharing of patient data through CliniShot complies with applicable confidentiality, professional council and privacy rules.
- Responding to patient requests for access, correction, deletion or portability of their data.

CliniShot does not collect or verify patient consent on behalf of healthcare professionals. The legal responsibility for lawful processing of patient data rests with the professional.

Failure to comply with these obligations may result in suspension or termination of the user's account, and the user assumes the corresponding legal liability for misuse of patient data.

18. Sharing Between Users

CliniShot offers controlled features to share clinical content with other healthcare professionals registered on the Service or with the patient. The user is responsible for ensuring that each share complies with this Policy and with applicable law.

The following actions are prohibited and may result in account suspension or termination:

- Sharing patient data without a valid legal basis.
- Disclosing or selling patient data to third parties.
- Sharing data with persons outside the medical professional context.
- Exporting, printing or storing data outside CliniShot's secure environment without adequate security measures.

CliniShot does not pre-screen the content shared between users. We may, however, take action when we become aware of sharing practices that violate this Policy or applicable law, including suspension of the sharing feature, suspension of the offending account, and reporting to authorities when legally required.

19. Cookies and Similar Technologies (Web)

Our web interface uses only strictly-necessary cookies, namely:

- Authentication and session cookies, used to keep you signed in.
- Security cookies, used to detect anomalous sessions and prevent fraud.
- Functional cookies, used to remember UI preferences (e.g., language).

We do not use advertising cookies, retargeting cookies or third-party analytics cookies on the web interface. If we ever introduce non-essential cookies, we will display a cookie consent banner with granular controls and update this Policy.

The mobile applications do not use cookies; they rely on local secure storage for authentication tokens and preferences.

20. Automated Decisions and Profiling

CliniShot does not take decisions that produce legal effects on data subjects based solely on automated processing. AI-assisted features are decision-support tools, and the healthcare professional remains the decision-maker. You may, at any time, request a human review of any output of an AI feature that affects you, by contacting support@clinishot.com.

21. Updates to This Policy

We may update this Policy from time to time. The “Last updated” date at the top of the document reflects the most recent version. When changes are material — for example, addition of a new sub-processor that processes clinical data, change in the legal basis of a processing activity, or change in retention periods — we will notify users in advance through an email to the address registered in the user's account.

Previous versions of this Policy are available upon request to support@clinishot.com.

22. Governing Law

This Policy is governed by Brazilian law. Any dispute arising out of or in connection with this Policy will be submitted to the courts of Rio de Janeiro, RJ, unless the user is entitled to a different forum by mandatory law (such as consumer protection law).

23. Acknowledgment of International Frameworks

CliniShot is a Brazilian company governed by LGPD. We acknowledge the existence of the EU GDPR and the U.S. HIPAA, and we have designed our practices to be broadly aligned with their principles where feasible. We do not, however, claim formal compliance with GDPR or HIPAA in this Policy. International users should review LGPD and consult their local rules; we are happy to answer specific questions at support@clinishot.com.

24. Contact

- Data Protection Officer: Gustavo Alexandre Monteiro da Silva
- General privacy and security inquiries: support@clinishot.com
- Postal address: Rua Barão de Saquarema, 379, Sala 03 Parte, Centro, Saquarema, RJ, CEP 28990-772, Brazil
- ANPD (Brazilian Data Protection Authority): www.gov.br/anpd

Thank you for trusting CliniShot with your data. We are committed to handling it with transparency, care and the highest level of protection we can apply.