A Brand of Nexnu Vision AI Solutions Pvt. Ltd.

PRIVACY POLICY

Effective Date: **6 February 2025**
Last Updated: **6 February 2026**
Version: **2.1**

This document is intended for public disclosure on nexclinai.com and governs the use of personal information by Nexnu Vision AI Solutions Pvt. Ltd.

1. Introduction

NexClinAI, operated by **Nexnu Vision AI Solutions Pvt. Ltd.** ("Company," "we," "our," or "us"), a company incorporated under the laws of India with its registered office at Madurai, Tamil Nadu, India, is committed to protecting your privacy and handling personal information responsibly.

This Privacy Policy explains how we collect, use, process, store, share, and safeguard information when you visit our website (nexclinai.com), use our services, or interact with our platform. It also describes your rights with respect to your personal data and how you may exercise them.

Our mission is to accelerate innovation in healthcare AI by providing curated, de-identified medical imaging datasets while upholding the highest standards of data privacy, ethical data sourcing, and regulatory compliance.

2. Scope of this Policy

2.1 What This Policy Covers

This Privacy Policy applies to:

- All visitors accessing nexclinai.com and its subdomains
- Individuals who register for our dataset portal or client accounts
- Clients evaluating, requesting, or licensing datasets from NexClinAI
- Hospital partners, research collaborators, and business partners
- Individuals subscribing to newsletters, attending NexClinAI webinars, or submitting inquiries through our contact forms
- Personnel of data partner institutions interacting with our ingestion or QC workflows

2.2 What This Policy Does Not Cover

This policy does not apply to:

- Patients or clinical subjects whose de-identified data may be included in research datasets curated by NexClinAI. All clinical datasets are de-identified prior to entering our processing environment and do not contain identifiable patient information.
- Third-party websites, services, or platforms linked from our website, each of which is governed by its own privacy policy.
- Data collected by external analytics or advertising services operating independently outside NexClinAI's direct control.

2.3 Regulatory Framework

This Privacy Policy has been drafted with reference to and in alignment with the following data protection frameworks:

- The Digital Personal Data Protection Act, 2023 (DPDP Act), India
- The Information Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India
- The General Data Protection Regulation (GDPR), European Union
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), United States
- Any other applicable national or regional data protection legislation in jurisdictions where our clients or data partners operate

3. Clinical Data Governance

3.1 No Direct Patient Data Collection

NexClinAI does not collect personal health information ("PHI") or personally identifiable information ("PII") directly from patients. We do not operate as a healthcare provider, a diagnostic facility, or a direct-to-patient data collector.

3.2 Data Sourcing

Clinical imaging datasets processed through our platform originate exclusively from licensed healthcare institutions, diagnostic imaging centres, and authorised data partners ("Data Partners"). These institutions are contractually responsible for:

- Ensuring lawful collection of clinical data under applicable regulations
- Obtaining any required patient consent or ethical approvals as mandated by their jurisdiction
- Performing or authorising de-identification of data prior to or upon transfer to NexClinAI

3.3 De-Identification Standard

Before any dataset is processed, curated, or made available to clients, it undergoes a structured de-identification procedure designed to remove all direct and indirect personal identifiers. Our de-identification practices are informed by internationally recognised standards, including but not limited to the HIPAA Safe Harbor method (removal of 18 specified identifiers) and GDPR anonymisation principles.

De-identification procedures include:

- Removal of identifiable metadata from DICOM headers and associated clinical records
- Pixel-level redaction of burned-in patient identifiers on medical images using our proprietary Redactor Pro tooling
- Automated and manual review cycles to detect and remediate residual personal information
- Chain-of-custody documentation to ensure traceability and auditability

3.4 No Re-Identification

NexClinAI does not attempt to re-identify individuals from de-identified datasets, nor does it permit or support any attempt by clients, partners, or any third party to do so. All dataset licensing agreements include explicit contractual prohibitions on re-identification. Any attempted or suspected re-identification constitutes a material breach and grounds for immediate termination of the data licensing arrangement, without prejudice to any other legal remedies available to NexClinAI.

3.5 Operating Models

NexClinAI supports two de-identification operating models depending on the Data Partner's requirements, privacy controls, and regulatory environment:

(a) Data Partner Transfer Model: The Data Partner transfers data via encrypted channels to NexClinAI's secure processing environment, where de-identification, QC, and curation are performed.

(b) On-Site De-Identification Model: De-identification is performed at the Data Partner's facility using NexClinAI-approved tools and procedures. Only validated, de-identified datasets are then transferred to NexClinAI.

4. Information We Collect

4.1 Information You Provide Directly

When you interact with NexClinAI through our website, contact forms, consultation bookings, or dataset request workflows, we collect information that you provide directly, such as:

- Full name
- Email address
- Phone number
- Organisation name, designation, and job title

- Country or region of operation
- Research interests, AI use case descriptions, or dataset requirements
- Correspondence content through email inquiries, meeting requests, or support communications

4.2 Information Collected Automatically

When you visit nexclinai.com, we automatically collect certain technical information through cookies, server logs, and analytics tools:

- IP address (which may be anonymised or truncated depending on configuration)
- Browser type, version, and language settings
- Device type, operating system, and screen resolution
- Pages visited, navigation paths, time spent on pages, and referral URLs
- Geolocation data (at country or city level, derived from IP address)

4.3 Information from Third-Party Sources

We receive information from third-party sources in certain business contexts, including:

- Publicly available professional profiles (e.g., LinkedIn) for business development purposes
- Referral information from existing clients or partners
- Information provided by Data Partners in connection with partnership onboarding

4.4 Information We Do Not Collect

NexClinAI does not collect:

- Personal Health Information (PHI) from patients
- Patient medical records, diagnoses, or treatment histories in identifiable form
- Biometric data, genetic data, or data concerning sexual orientation
- Financial account details, credit card numbers, or banking information directly. Payment processing, where applicable, is handled by third-party payment processors.

5. How We Use Your Information

We use the information we collect for the following purposes:

Service Delivery

To provide access to datasets, process licensing requests, respond to inquiries, manage client accounts, facilitate dataset delivery, and support research collaborations.

Communication

To send relevant updates about NexClinAI services, respond to consultation requests, deliver service notifications, and provide information about new dataset offerings, platform features, or events. Marketing communications are sent only with your consent and include an unsubscribe mechanism.

Business Operations

To manage invoicing, enforce contractual obligations, maintain internal records, conduct compliance processes, perform business analytics, and improve service quality.

Security and Fraud Prevention

To monitor system activity, detect unauthorised access or suspicious behaviour, protect our infrastructure and intellectual property, and ensure the integrity of client data.

Legal and Regulatory Compliance

To comply with applicable laws, respond to lawful requests from regulatory or law enforcement authorities, enforce our Terms and Conditions, and protect our legal rights.

Platform Improvement

To analyse website usage patterns, improve user experience, optimise website performance, and develop new features or service offerings.

6. Legal Basis for Processing

6.1 Under GDPR (EEA/UK Users)

For individuals located in jurisdictions governed by the General Data Protection Regulation, NexClinAI relies on the following legal bases for processing personal data:

Processing Purpose	Legal Basis
Service delivery and contract performance	Necessity for the performance of a contract (Art. 6(1)(b))
Communication and marketing	Legitimate interest (Art. 6(1)(f)) or consent (Art. 6(1)(a))
Website analytics and improvement	Legitimate interest (Art. 6(1)(f))
Regulatory and legal compliance	Legal obligation (Art. 6(1)(c))
Research collaboration onboarding	Consent (Art. 6(1)(a))
Security and fraud prevention	Legitimate interest (Art. 6(1)(f))

6.2 Under DPDP Act (Indian Data Principals)

For individuals whose data is processed under the Digital Personal Data Protection Act, 2023, NexClinAI processes personal data based on consent obtained from the Data Principal, or for legitimate uses as prescribed under Section 7 of the Act.

7. Data Sharing and Disclosure

NexClinAI does not sell, rent, or trade your personal information.

We share information only under the following limited and controlled circumstances:

Trusted Service Providers

We engage vetted third-party service providers who assist in operating our business. These providers are contractually bound to process data only as instructed by NexClinAI and to implement appropriate security measures. Categories include secure cloud hosting, analytics, email communication platforms, scheduling tools, and customer support systems.

Legal and Regulatory Requirements

We disclose personal information only when required by law, in response to valid legal process (such as a court order, subpoena, or government request), or when necessary to protect our legal rights, enforce our Terms, or respond to an emergency involving personal safety.

Business Transfers

In the event of a merger, acquisition, reorganisation, or sale of all or a portion of our assets, personal information may be transferred as part of the transaction, subject to the transferee agreeing to protect your information consistent with this Privacy Policy.

Clinical Datasets

Medical datasets provided to clients and research collaborators are fully de-identified prior to transfer and do not contain personal health information. The disclosure of de-identified datasets does not constitute sharing of identifiable personal data under applicable data protection laws.

8. International Data Transfers

NexClinAI collaborates with research institutions, AI developers, CROs, and healthcare technology companies across multiple countries including but not limited to the United States, European Union member states, the United Kingdom, and other jurisdictions.

Where datasets or personal information are transferred internationally:

- Only de-identified and anonymised clinical datasets are transferred to international partners. No personally identifiable patient information is exported.
- For personal data of website users or clients, appropriate safeguards are implemented, which may include Standard Contractual Clauses (SCCs) approved by the European Commission, adequacy decisions, or other lawful transfer mechanisms.
- All international data partners and clients are bound by contractual restrictions prohibiting re-identification of individuals and unauthorised use of datasets.

9. Data Security

Protecting information is a core operational priority for NexClinAI. We implement a multi-layered approach combining technical, administrative, and physical safeguards:

Technical Safeguards

- AES-256 encryption for data at rest
- TLS 1.2+ encryption for data in transit
- Secure cloud infrastructure with geographically distributed redundancy
- Multi-factor authentication (MFA) for all internal systems and client portals
- Network segmentation, intrusion detection systems, and firewalls
- Automated vulnerability scanning and patch management

Administrative Safeguards

- Role-based access control (RBAC) with principle of least privilege
- Comprehensive activity monitoring and audit logging
- Mandatory data handling and privacy training for all personnel
- Vendor security assessments and due diligence for all third-party service providers
- Documented incident response procedures

Breach Notification

In the unlikely event of a personal data breach, NexClinAI will:

- Investigate and contain the breach promptly
- Notify affected individuals and relevant supervisory authorities in accordance with applicable legal timeframes (72 hours under GDPR; as prescribed under DPDP Act)
- Document the breach and remediation steps taken

10. Data Retention

We retain personal information only for as long as necessary to fulfil the purposes for which it was collected, to comply with legal obligations, resolve disputes, and enforce our agreements.

Data Category	Retention Period	Basis
Website analytics	Up to 26 months	Legitimate interest
Client records and contracts	Duration of relationship + 7 years	Legal and contractual obligation
Technical and server logs	Up to 6 months	Security and operational necessity
Marketing and communication records	Until consent is withdrawn	Consent
Inquiry and consultation records	Up to 3 years after last interaction	Legitimate interest
De-identified clinical datasets	As per licensing agreement terms	Contractual obligation

Upon expiration of the applicable retention period, personal data is securely deleted or anonymised such that it can no longer be associated with an identified or identifiable individual.

11. Your Privacy Rights

Depending on your jurisdiction and applicable data protection laws, you may be entitled to exercise the following rights:

Under GDPR (EEA/UK)

- Right of Access (Art. 15): Obtain confirmation of whether we process your data and request a copy.
- Right to Rectification (Art. 16): Request correction of inaccurate or incomplete data.
- Right to Erasure (Art. 17): Request deletion of your personal data ("right to be forgotten") subject to applicable exceptions.
- Right to Restriction (Art. 18): Request restriction of processing under specified circumstances.
- Right to Data Portability (Art. 20): Receive your data in a structured, commonly used, machine-readable format.

- Right to Object (Art. 21): Object to processing based on legitimate interest, including profiling.
- Right to Withdraw Consent: Where processing is based on consent, withdraw at any time without affecting the lawfulness of prior processing.
- Right to Lodge a Complaint: File a complaint with a supervisory authority in your jurisdiction.

Under DPDP Act (India)

- Right to access information about personal data processing
- Right to correction and erasure of personal data
- Right to grievance redressal
- Right to nominate a representative

To exercise any of these rights, please contact our Data Protection Officer at the address provided in Section 17 below. We will respond to verifiable requests within the timeframes prescribed by applicable law (generally 30 days under GDPR).

12. Cookies and Tracking Technologies

12.1 Types of Cookies Used

Our website uses cookies and similar tracking technologies to support functionality, performance, analytics, and marketing. The categories of cookies we use are:

Cookie Category	Purpose	Duration
Strictly Necessary	Essential for site functionality, session management, and security	Session / Persistent
Preferences	Store user preferences such as language or display settings	Up to 12 months
Analytics / Statistics	Understand usage patterns, page performance, and visitor behaviour	Up to 26 months
Marketing	Track user activity across sites for advertising and retargeting purposes	Up to 24 months

12.2 Cookie Consent

Our website implements a cookie consent management tool (powered by Complianz). Upon your first visit, the consent tool presents you with the option to accept or decline non-essential cookies. Strictly necessary cookies cannot be disabled as they are required for the basic operation of the website. You can change your cookie preferences at any time through the cookie settings link available in the website footer.

12.3 Browser Controls

You may also manage cookies through your web browser settings. Please note that disabling certain cookies may affect the functionality and performance of our website. For Google Analytics, you may opt out using the Google Analytics Opt-out Browser Add-on.

13. Third-Party Services

NexClinAI relies on trusted external service providers to support business operations. These providers are selected based on their security posture, compliance credentials, and data handling practices. Current third-party services include, but are not limited to:

Service Provider	Purpose
Amazon Web Services (AWS)	Secure cloud infrastructure and data hosting
Cloudflare	Website security, DDoS protection, and CDN
Google Analytics	Website usage analytics and visitor insights
Calendly	Consultation and meeting scheduling
Zoom	Video conferencing for client consultations
Mailchimp	Email marketing and newsletter distribution
GitHub	Version control and development collaboration

Each provider maintains its own privacy policy governing how information is processed on their respective platforms. NexClinAI is not responsible for the privacy practices of third-party services. We encourage users to review the privacy policies of any third-party services they interact with through our platform.

14. Children's Privacy

NexClinAI services are designed for business-to-business use and are not directed at individuals under the age of 18 (or the applicable age of majority in the relevant jurisdiction). We do not knowingly collect personal information from minors.

If we become aware that we have inadvertently collected personal data from a minor, we will take prompt steps to delete such information. If you believe a minor has provided us with personal information, please contact our Data Protection Officer immediately.

15. Automated Decision-Making and Profiling

NexClinAI does not engage in fully automated decision-making or profiling that produces legal effects or similarly significant effects on individuals without human oversight.

Our internal data processing pipelines (including QC automation, duplication detection, and modality classification) operate exclusively on de-identified clinical datasets and do not process personal data of website users or clients in an automated decision-making capacity.

16. Contact Information

For any questions, concerns, or requests regarding this Privacy Policy, your personal data, or NexClinAI's data handling practices, please contact:

Nexnu Vision AI Solutions Pvt. Ltd.

Operating as: **NexClinAI**

Registered Office: Madurai, Tamil Nadu, India

Contact Type	Details
Data Protection Officer	privacy@nexclinai.com
General Inquiries	info@nexclinai.com
Legal and Compliance	legal@nexclinai.com
Technical Support	support@nexclinai.com
Website	https://nexclinai.com

We aim to acknowledge all privacy-related inquiries within 48 hours and provide a substantive response within 30 days.

17. Grievance Officer (India)

In accordance with the Information Technology Act, 2000 and the rules made thereunder, and the DPDP Act, 2023, the details of the Grievance Officer are as follows:

Name: **The Data Protection Officer, NexClinAI**

Email: privacy@nexclinai.com

Address: Nexnu Vision AI Solutions Pvt. Ltd., Madurai, Tamil Nadu, India

The Grievance Officer shall acknowledge the receipt of any complaint or grievance within 48 hours and shall resolve the same within 30 days from the date of receipt.

18. Changes to This Privacy Policy

NexClinAI reserves the right to update or modify this Privacy Policy at any time to reflect changes in our data practices, regulatory requirements, or operational needs.

Material changes will be communicated through one or more of the following channels:

- A prominent notice on the nexclinai.com website
- Email notification to registered users and active clients
- An updated “Last Updated” date at the top of this document

We encourage you to review this Privacy Policy periodically. Your continued use of NexClinAI’s website or services following the posting of changes constitutes your acknowledgment of such changes. Archived versions of previous policies may be requested by contacting our Data Protection Officer.

19. Governing Law and Jurisdiction

This Privacy Policy shall be governed by and construed in accordance with the laws of India. Any disputes arising out of or in connection with this Privacy Policy shall be subject to the exclusive

jurisdiction of the courts at Madurai, Tamil Nadu, India, without prejudice to your right to lodge a complaint with a supervisory authority in your jurisdiction under applicable data protection laws.

20. Acknowledgment

By accessing the NexClinAI website, registering for our services, or engaging with our platform in any capacity, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy. If you do not agree with any provision of this policy, please discontinue your use of our website and services.

— End of Privacy Policy —

Document Version 2.1 | April 2026 | NexClinAI