

Privacy Policy

Effective Date: January 1, 2025

Last Updated: February 20, 2026

1. Introduction

MyCyber Clinics (“we,” “our,” or “us”) is committed to protecting the privacy, security, and confidentiality of all users (“you,” “your”) who access our telehealth services through our website or mobile application.

This Privacy Policy explains how we collect, use, process, store, protect, and disclose your personal and medical information.

By accessing or using MyCyber Clinics, you acknowledge that you have read, understood, and agreed to this Privacy Policy.

If you do not agree, please discontinue use of our services.

2. Information We Collect

We collect only the information necessary to provide secure and effective telehealth services.

A. Personal Information

(Collected with your explicit consent)

- Full Name
- Date of Birth / Age
- Gender
- Contact details (Email, Phone Number, Address)
- Government-issued identification (where verification is required)

B. Health Information

(Securely processed and encrypted)

- Medical history
- Symptoms and health complaints
- Diagnoses and prescriptions

- Consultation records and doctor notes
- Diagnostic test results
- Uploaded medical documents or files

Health information is classified as **sensitive personal data** and receives enhanced protection.

C. Device & Usage Information

- Device type and operating system
- Browser type and app version
- IP address and general location (if enabled)
- Cookies and analytics data for performance and security

Google Play Compliance

We collect and process only data necessary to provide core telehealth services.

We do **not** collect or use personal data for unrelated purposes or advertising.

3. How We Use Your Information

We use your information lawfully and responsibly to:

- Provide secure telehealth consultations
- Schedule and manage appointments
- Process and confirm payments securely
- Improve platform functionality and user experience
- Maintain security and prevent fraud
- Comply with medical, legal, and regulatory requirements

Anonymized Research & Public Health Monitoring

We may use **de-identified and anonymized medical data** solely for:

- Educational research
- Monitoring population-level health trends
- Designing public health interventions
- Improving healthcare access and service quality

No identifiable personal information is ever disclosed for research purposes.

Important Assurance

We do **not** use your personal or health data for marketing or advertising.

4. Information Sharing & Disclosure

We do **not** sell your personal data.

We may share information only under the following circumstances:

A. With Licensed Healthcare Professionals

To provide consultation, follow-up care, referrals, or medical coordination.

B. With Trusted Third-Party Service Providers

(Restricted and Controlled Access)

- Secure cloud hosting providers
- Payment processing gateways
- Encrypted communication tools
- Analytics platforms for service improvement

All partners are bound by strict data protection and confidentiality agreements.

C. Legal & Regulatory Requirements

We may disclose information when required:

- By law, court order, or lawful government request
- To prevent fraud, data breaches, or harm
- To protect patient safety

Google Play Compliance

All third-party access and data processing practices are disclosed in line with [Google Play's Data Safety Policy](#).

5. Your Rights & Choices

You have full control over your personal data.

You may:

- **Access & update** your personal information
- **Request Data Deletion** of your account and stored records

- **Withdraw Consent** for non-essential processing
- **Restrict Tracking** through cookie settings
- **Request Data Portability** where legally applicable

Sensitive health data is processed only with explicit user consent, in accordance with [Google Play's User Data Policy](#).

6. Data Security Measures

We implement industry-standard safeguards to protect your information:

- End-to-End Encryption for calls, chats, and records
- Multi-Level Access Controls (role-based permissions)
- Secure server infrastructure
- Regular security audits and compliance reviews
- Incident response protocols for breach management

We do not make deceptive or unverifiable security claims.

7. Health Data Compliance

MyCyber Clinics adheres to applicable data protection and medical privacy regulations, including:

- **NDPR (Nigeria Data Protection Regulation)**
- **HIPAA (U.S. users, where applicable)**
- **GDPR (European Union users)**
- **African Union Data Protection Guidelines**

We accurately declare all health data processing practices under Google Play's Health Apps Policy.

8. Cookies & Tracking Technologies

We use cookies for:

- **Essential Functions** – required for platform operation
- **Analytics & Performance** – to improve service (opt-out available)

You may manage cookies through your browser or device settings.

9. Data Retention & Deletion

We retain personal and health data only for as long as necessary to:

- Provide services

- Meet regulatory requirements
- Fulfill legal obligations

You may request account deletion at any time by contacting us.

Upon deletion:

- Data is securely erased, or
- Anonymized beyond recovery where legally required

Our retention practices align with [Google Play's User Data Retention Guidelines](#).

10. International Data Transfers

Your data may be stored on secure servers located outside Nigeria.

All international transfers comply with recognized legal safeguards, including:

- GDPR Standard Contractual Clauses
- Equivalent lawful transfer mechanisms

11. Policy Updates

We may update this Privacy Policy to reflect:

- Regulatory changes
- Platform improvements
- Security updates

Users will be notified through:

- In-app notifications
- Email (where provided)

Continued use of the platform after updates indicates acceptance.

12. Contact Information

For privacy inquiries, data access requests, or complaints, contact:

Email: support@mycyberclinics.com

Phone: +234 707 321 3692

Final Acknowledgment

By using MyCyber Clinics, you confirm that:

- You have read and understood this Privacy Policy
- You consent to the collection and use of your data as described
- You understand your rights and how to exercise them